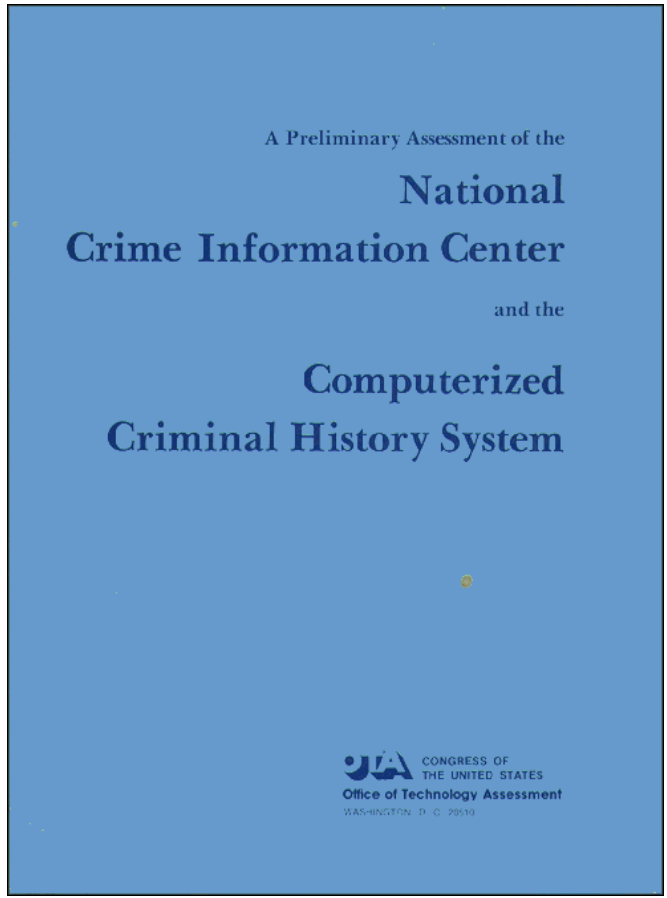
A Preliminary Assessment of the National Crime Information Center and the Computerized Criminal History System

December 1978

NTIS order #PB-291845





Library of Congress Catalog Card Number 78-600164

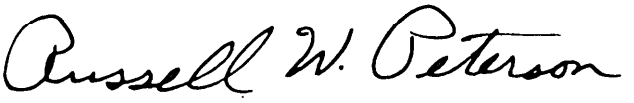
For sale by the Superintendent of Documents, U.S. Govement Printing office
Washington, D.C. 20402 - Price $2.75

FOREWORD

In recent years, the application of computer and communications technology to criminal justice systems has increasingly drawn the attention of Congress. Such concern is exemplified by requests from the House and Senate Committees on the Judiciary that OTA undertake an assessment of the Department of Justice's National Crime Information Center and the Computerized Criminal History System.

This report, a background planning document for that assessment, identifies and analyzes some major issues in the future development of this FederaI-State system. These are: the information needs for administering criminal justice programs and assuring constitutional rights; federalism, including division of authority, and cost apportionment; organization, management, and oversight; the planning process, and social impacts such as the effects on the administration of justice and the creation of a dossier society. Many of the policy and technical concerns discussed in the report are common to other major national information systems being assessed by OTA in the National Information Systems Study which addresses, in addition to the National Crime Information Center, electronic funds transfer and electronic mail.

The following background report was prepared by the Office of Technology Assessment with the assistance of an ad hoc interdisciplinary working group of experts in law, public administration, State and local criminal justice and law enforcement, computer sciences, civil liberties, and other related areas.



RUSSELL W. PETERSON
Director

OTA Project Staff
National Crime Information Center's Computerized Criminal History System

Iram J. Weinstein, Project Director

Marcia J. MacNaughton — Phil Hirsch

Barbara Balbiani — Liz Emanuel

Robert F. Daly, Coordinator

OTA Publishing Staff

John C. Holmes, Publishing Officer

Kathie S. Boss — Joanne Heming

Working Group Members

Adam D'Alessandro
Acting Deputy Commissioner
New York State Division of Criminal Justice Services
Albany, N.Y.

Jerry J. Berman
Legislative Counsel
American Civil Liberties Union
Washington, D.C.

Donald G. Ingraham
Office of the District Attorney
Oakland, Calif.

Steve Kolodney
Executive Director
SEARCH GROUP, Inc.
Sacramento, Calif.

Kenneth Laudon
Professor
John Jay College of Criminal Justice
New York City, N.Y.

Charles Lister
Attorney at law
Covington & Burling
Washington, D.C.

Michael D. Maltz
Professor, Department of Criminal Justice
University of Illinois at Chicago Circle
Chicago, Ill.

Jeffrey A. Meldman
Professor
Sloan School of Management
Massachusetts Institute of Technology
Cambridge, Mass.

Brian Ruder
Information Science Laboratory
SRI International
Stanford Research Institute
Menlo Park, Calif.

James J. Zurawski
Assistant Deputy Superintendent
Research, Development, and Data Systems Division
Chicago Police Department
Chicago, 111.

David T. Stanley
Consultant
Vienna. Va.

Note: The working group members provided advice and critique, but do not necessarily approve, disapprove, or endorse the report, for which OTA assumes full responsibility.

CONTENTS

Chapter *Page*

1. Summary 3

2. Background 7

   National Crime Information Center System 7
   Committee Requests. 8
   History and Perspectives 9
   The Present Situation. 12

3. Issues 17

   Information Needs 17
      Criminal Justice Requirements 17
      Constitutional Rights.. 20
   Federalism 25
      Division of Authority. 25
      Cost Apportionment. 27
   Organization, Management, and Oversight 29
      Management Responsibilities 29
      Oversight 31
      Managing Agency 33
   The Planning Process. 35
      Participation in Planning 35
      Technical Alternatives 37
      Transition Planning 40
   Social Impacts 44
      Effects on the Criminal Justice System 44
      The Dossier Society 46
      Privacy and Civil Liberties Trends 47

Appendix A—Letters of Request 51

Appendix B—Pertinent Excerpts From the Department of Justice Report 68

Appendix C—Chronology of CCH 77

Appendix D—Glossary 81

CHAPTER 1

Summary

CHAPTER 1

Summary

The National Crime Information Center (NCIC) is a nationwide information network operated by the Federal Bureau of Investigation (FBI) since 1967 which provides criminal justice agencies throughout the country with access to information on stolen vehicles and other stolen property, wanted persons, and missing persons. In 1971, a Computerized Criminal History (CCH) file was added, containing records of individual offenders' criminal histories. The CCH program has been slow to develop; only 12 States and the Federal Government contribute records to the system.

Although questions have been raised regarding the effectiveness of the entire NCIC network, CCH has been the most controversial aspect of the system. The controversy over CCH has focused on the question of whether the FBI should be authorized to provide a message-switching service to route inquiries and responses regarding criminal history information between States. However, this question rests on broader issues, including the system's potential impact on constitutional rights of citizens and on the relationships between the Federal and State governments in the administration of criminal justice. The possible longer term impacts of the system on society, both desirable and undesirable, have also been the subject of speculation. Because of these and other major concerns, the Office of Technology Assessment (OTA) was asked by the Judiciary Committees of the House and the Senate to undertake an assessment of the NCIC system, with emphasis on the CCH portions.

This report is the result of a preliminary effort by the OTA staff and an ad hoc working group of experts to assess the critical issues raised by CCH and to identify the important questions regarding each issue. As a preliminary effort, the document systematically identifies issues but does not try to answer the questions they raise.

Although CCH has been the subject of numerous studies, conferences, and hearings, there is only limited information regarding the ways in which law enforcement and the criminal justice decisionmakers as well as other government and private individuals and the press make use of criminal history information, its benefits, the value of nationwide access to this information, and the value of rapid access. Even more limited is information on the quality of criminal history records in terms of completeness, accuracy, and currency, and the effects of inadequate quality on decisionmaking and constitutional rights of individuals involved. It must be recognized that computerization can eliminate certain kinds of errors which plague manual records. No computerized information system is perfect. Since, with computers, increased transaction volumes are to be expected, the potential for harm from dissemination of inaccurate or incomplete records also increases.

Much better information is needed concerning these and other questions raised in the report in order to make assessment and evaluation of the policy alternatives regarding CCH.

Because of the decentralized nature of the U.S. criminal justice system and because the generation and use of criminal history information occurs mostly at the State and local levels of government, the States have a primary stake in establishing standards and procedures for the keeping and dissemination of criminal history information. On the other hand, minimum national standards also are required for an interstate CCH system. Attempts at comprehensive Federal legislation to control the collection and dissemination of criminal justice information have failed to produce legislation or a consensus as to how authority for this important area of control of the system should be allocated between the States and the Federal Government. The lack of resolution of this issue is a very serious obstacle to the successful development of CCH. This federalism issue underlies issues raised in the report with regard to management, oversight, and planning process for the system.

The role of the FBI as a manager of the CCH system should be raised as an issue for further

examination. By some standards, the FBI is uniquely qualified to run the CCH program; they have the cooperation and respect of law enforcement agencies throughout the country; they have an extensive fingerprint identification function, which is necessary to support effective use of CCH where identity is in question; and the transfer of the CCH system to some other Government agency might be viewed with great alarm by the law enforcement community. By other standards, and in light of changing public attitudes towards privacy, civil liberties, and governmental controls, the FBI is placed in a position of great conflict of interest in bearing these records management responsibilities in addition to its primary investigatory responsibilities. An argument can be made that higher public confidence would be attained by placing CCH operations in a more neutral agency.

The Computerized Criminal History system is now undergoing an extensive review in Congress, in the Justice Department, and in the States. Thus an important and immediate issue is how to accommodate the needs and interests of the various levels of government, the Criminal Justice Community, and other stakeholder groups in the planning process. Although some Federal agencies use it, the essence of the CCH system is that primary sources and users of the data are the State and local criminal justice agencies. The history of CCH development has shown the importance of the States participation in the planning process. It is questionable that a blueprint for a workable system can be created without their playing a direct, perhaps even principal role in the planning, including participation by a cross-section of interest groups who will be affected by the system.

In rethinking the CCH system, a number of technical system alternatives should be considered. Alternative approaches to managing message traffic are available that might relieve some of the concerns raised about the FBI message-switching plan, while raising questions of their own regarding costs and auditability. Again the federalism issue is important. Those who see the responsibility for maintaining and disseminating criminal history records as falling primarily with the States argue for viewing CCH as many different State systems with a need to exchange information, not necessarily through NCIC. Those who see a strong need for Federal oversight and Federal standards for information dissemination argue for a centrally managed system.

In a future full-scale assessment, OTA will examine these issues, the policy alternatives available, and their long-range implications for society.

CHAPTER 2

Background

CHAPTER 2

Background

NATIONAL CRIME INFORMATION CENTER SYSTEM

The National Crime Information Center (NCIC) is a national system, managed and operated by the Federal Bureau of Investigation (FBI) which uses computers and telecommunication technology for transferring and sharing criminal justice information among Federal, State, and local agencies. The center is physically located in the FBI's computer facility in Washington, D.C. and includes a telecommunication network that reaches automated or manual teletype terminals in all of the .50 States, the District of Columbia, Canada, Puerto Rico, and some large cities. The service of NCIC is free to the participating States and the funds for it come from the FBI's authorization.

In addition to the Computerized Criminal History (CCH) system, which is the subject of this report, NCIC has eight files containing information about wanted persons, missing persons, stolen vehicles, and other missing property. The summary information in these files is available online in response to inquiries from law enforcement agencies throughout the country. Confirmation of the validity of the data and further details must be obtained from the agency that originated the record. Each State has a single control terminal connected to the NCIC computer in Washington through which all inquiries and record updates must be transacted. At the present time, there are well over 6,000 law enforcement terminals connected to NCIC, averaging over 250,000 transactions daily.

The CCH file was added to NCIC in 1971, following a successful demonstration of feasibility sponsored by the Law Enforcement Assistance Administration (LEAA). Originally conceived as an index file, pointing to records held in State repositories, the system, as implemented in NCIC, stores full details of criminal records that are supplied by the States and the Federal Government.

The CCH file now makes available instantly, more than 1,287,642[1] criminal histories of people who at one time or another have been arrested on certain felony and misdemeanor charges which have been established as "criterion offenses. "

After 6 years of slow development, and despite heavy Federal funding of State systems by LEAA, only 12 States in addition to the Federal Government are contributing records to this national data bank for use by their own agencies, by other State agencies, and by Federal agencies. Two of the earliest States to develop CCH programs, New York and Pennsylvania, withdrew from the system in 1974, finding that they could not justify the cost of updating the duplicate records held by NCIC.

Despite this slow development, criminal justice practitioners are virtually unanimous in their view that interstate exchange of criminal history information is necessary for the efficient and effective administration of justice. State officials express the view that implementation of CCH has been slowed by indecisiveness and confusion on the part of the Federal Government.

[1]August, 1978 NCIC *Newsletter.*

COMMITTEE REQUESTS

This preliminary analysis was conducted as an initial planning activity in response to a request for an assessment of NCIC made by the Chairman of the House Committee on the Judiciary, Representative Peter Rodino, and the Chairman of the Subcommittee on Civil and Constitutional Rights, Representative Don Edwards.

They were joined in this request by the Chairman of the Senate Committee on the Judiciary, Senator James O. Eastland, and the Chairmen of two Judiciary Subcommittees, the Subcommittee on Administrative Practice and Procedure chaired by Senator James Abourezk, and the Subcommittee on the Constitution, chaired by Senator Birch Bayh.

As part of its legislative and oversight responsibilities for the Federal Bureau of Investigation of the Department of Justice, the House Subcommittee is studying the FBI's criminal justice information systems. Assuring proper standards for these systems has been the legislative concern of the subcommittee for the last three Congresses. Attention has been focused on cost-effectiveness, efficiency, security, and privacy protection. In addition, the larger issue of the role of the Federal Government in this exchange of information by and for local law enforcement agencies has been raised before the subcommittee.

In seeking OTA's help, the House Chairman cites* the technical complexity of nationwide computerized information and telecommunications systems, and the Justice Department's work on a proposal with both short- and long-range plans for the future of NCIC, the FBI's role in law enforcement telecommunications systems, and message switching generally. He cites a number of provisions that would necessarily have to be addressed in the FBI's plans for the future of NCIC: appropriate privacy and security measures and safeguards for constitutional rights and liberties; the needs of the primary users, the States; and the right balance between State and Federal control.

The Senate Judiciary Committee has been similarly concerned for several Congresses with the legislative and oversight issues raised by the NCIC, particularly the CCH files. Yet the chairman notes that it has not had the benefit of a thorough evaluation of exactly what information is in the system, who needs it and why.

In addition to the matters covered by the House request, the Senate Committee asks* for emphasis on several issues, including: the impact of the interrelationship of many information policies that govern the administrative practices of the Federal and State agencies that use or are affected by NCIC, particularly by the criminal history records; the effect of any NCIC changes on other Federal agency users, as well as others who use CCH/NCIC files; and the relationship of NCIC programs, operation, and controls to the constitutional separation of powers and the independence of the Judiciary.

The Chairman also cited the benefits which might be gained from such a study; not only to improve the efficiency of NCIC, but to help Congress in its consideration of other proposals for applying such technology on a nationwide basis:

> We believe Congress will benefit from OTA's assessment of NCIC. This system represents the first and most important nationwide use of computer and telecommunications technology to link Federal, State, and local governments, and to apply the technology to serious law enforcement and criminal justice problems of concern to our entire society. Many of the issues involved in NCIC are those common to any such Federal-State information systems.

An assessment of this large Federal-State personal information system would also partially respond to concerns expresed in 1976 and 1977 in letters to the Director of OTA from two different Chairmen of the Subcommittee on Government Information and Individual Rights of the House Government Operations Committee. , They have cited the subcommittee's assignment involving the field of computer technology and other means of electronic communications, which flows from its legislative jurisdiction,

● See appendix A.

*See appendix A.

particularly from the mandates of the Privacy Act of 1974 and the Freedom of Information Act.

The current Chairman, Representative Richardson Preyer, reconfirmed the subcommittee's earlier request for assistance on this issue, but commented "Of equal, if not greater importance is the subcommittee's concern over the impact of technological advances in the development of government information programs in general ."

HISTORY AND PERSPECTIVES

The CCH information system is rooted in all the complex historical relationships among governments and institutions which have characterized our Federal system from its beginning, particularly in the area of law enforcement.

To the extent it is a system, CCH was developed and superimposed over patterns, relationships, processes, and ways of making decisions in many hundreds of different political arenas in every State. It was introduced into a framework already set by constitutional, statutory, judicial, and administrative doctrines. Although it was meant to be an eventual substitute for the pre-existing slower arrangements for sharing information at the Federal level, it has suffered the drawbacks of operating both as a parallel system, as a supplement to the old arrangement, or in competition with it as the older system was developed and expanded with new technologies.

For these reasons, the development of the CCH data-sharing program appears to have been caught up in the same kinds of political struggles and issues, often with new labels, which have dominated the old relationships. The decision areas for CCH development have, for some purposes, merely provided more points of access for those contending forces. In addition, CCH has brought into the old discussions newer forces with varied professional, economic, and organizational interests in the application of information sciences and computer and telecommunications technology.

The origin of the application of automated data-processing (ADP) technology to the exchange of criminal history records is grounded in the political agendas of the decade of the sixties, where political contenders debated the issues of law and order and proposed different kinds of remedies for dealing with crime in a highly mobile society. It was conceived in a time of considerable social unrest, of protest activity, demonstrations, dissent, and violence, frequently involving travel across State lines for the purpose. Law enforcement officials and courts were often confronted with multiple arrests which placed strains on information and investigative resources and on the capacity of their criminal justice systems to administer due process of law. Organized crime elements, active in interstate commerce raised other public and government concerns. The extent of the day-to-day problems of crime in the community were beginning to show up as information technology enabled better crime reporting.

These public concerns coincided with trends in developing and applying computer and telecommunications technology to deal more efficiently and economically with problems of government and society. Tandem with this was the enthusiasm over the systems approach to public administration.

These movements and trends flowered in the report of the 1967 Commission on Law Enforcement and the Administration of Justice appointed by President Johnson. A landmark in the intellectual history of criminal justice issues, the Commission report recommended applying a systems approach to those interrelated problems through computer technology. It called for "a national law enforcement directory that records an individual's arrest for serious crimes, the disposition of each case, and all subsequent formal contacts with criminal justice agencies related to those arrests. "

Following passage of the Safe Streets Act of 1968, the Department of Justice's LEAA, through Project SEARCH (System for Electronic Analysis and Retrieval of Criminal Histories), an interdisciplinary group, sponsored an experi-

36-738 O - 78 - 3

ment to develop a plan for collecting and sharing the records of people involved in the administration of criminal justice.

The early Project SEARCH reports on the need for privacy, confidentiality, and security in the new systems addressed the social and political concerns being expressed in Congress and elsewhere in the Nation about the ways of achieving a just and fair society, accountability in government, how to prevent unwarranted surveillance and other invasions of privacy, and how to combat crime effectively. Principles were laid down concerning data content, rules of access and data use, dissemination, rights of challenge and redress, and administration.

LEAA began funding the development of State information technology that would enable States to computerize their files and participate in the system. By congressional mandate, they also began developing legislation to provide standards for information systems that they funded. In 1973, Congress amended the Safe Streets Act of 1968 to require that all criminal history information collected, stored, or disseminated through LEAA support shall contain, to the maximum extent feasible, disposition as well as arrest data where arrest data is included. These activities are to take place under procedures reasonably designed to ensure that all such information is kept current; the Administration shall assure that the security and privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes. In addition, an individual who believes that criminal history information contained in an automated system is inaccurate or incomplete is entitled to review and correct it.

During the 92d, 93d, and 94th Congresses the House Judiciary Subcommittee on Civil and Constitutional Rights and the Senate Judiciary Subcommittee on Constitutional Rights held hearings on the various legislative proposals to set privacy, confidentiality, and security standards for arrest records and for any Federal or federally supported criminal justice information systems.

Testimony included that of Federal and State law enforcement officials and administrators involved in many different criminal justice programs; groups concerned with protection of privacy and civil liberties: spokesmen for press, radio, and television interests concerned with unfettered access to information; constitutional law experts concerned with accountability in government; computer professionals; State officials concerned with demands and controls that would be placed on standards and uses of computer technology, and particularly on State computer operations; representatives from business, industry, and other organizations who used arrest records; and many others concerned with the effects on rights to due process of law under current practices as well as the range of possibilities for affecting such rights in future programs.

During these congressional studies, according to one expert observer, five major issues dominated the agenda:[z]

1. What general rules if any should be set by Federal law to restrict the exchange of criminal justice information between criminal justice agencies?
2. What general rules should govern the release of criminal justice information outside the criminal justice community?
3. The extent, if any, of sealing or purging of records?
4. What rules should govern the collection and exchange of criminal justice intelligence and investigative files? and
5. Who should administer any Federal legislation—the Attorney General or a Board composed of private citizens and representatives of the States and Federal Government?

The problem of how to set controls on intelligence and investigative information with other criminal justice arrest records was a particularly difficult legislative task. Some congressional sponsors of legislation and many witnesses felt that it would be impossible and unwise to set specific standards for collection and dissemination of criminal history records without any statutory controls on dissemination of more sensitive and potentially damaging intelligence information which Federal and State agencies maintained about people.

The extensive congressional hearings on this draft legislation produced a high degree of co-

[z] Mark Gitenstein, address before the International Search Symposium, 1975.

operation between Congress and the executive branch, and among Federal and State law enforcement and criminal justice officials, press and media, civil liberties representatives, and other interested parties. However, no consensus could be reached which was strong enough to support final passage of legislation specifically to control law enforcement and criminal justice records. This was connected to and reinforced by the fact that the Justice Department undertook to draft regulations to reflect the consensus already developed and to set privacy and security standards for routine exchange of criminal history information by the FBI as well as for the federally funded criminal history record systems at the State and local level.

The further development of a national consensus on what the public demands from official information systems was fueled by a Department of Health, Education, and Welfare (HEW) Report on records on computers in early 1974 which summarized many of the current concerns about fairness and accuracy in government information programs and use of personal records, The report called for an application of "fair information practices" in the management of all personal records systems, including procedures for access, challenge, and rebuttal, for keeping data accurate and current and controlling improper dissemination. However, the scope of its recommendations generally excluded law enforcement and criminal justice records.

The report's findings encouraged the introduction of bills in many State legislatures and in Congress.

In Congress, such bills were introduced and the Senate and House Government Operations Committees held hearings on what was to become the Privacy Act of 1974. This statute, for the first time, established broad management principles and standards for the protection of privacy, confidentiality, and security in the Federal Government's computerization, collection, management, use, and disclosure of personal information about individuals.

In considering the scope of the act, the committees took note of the pending criminal justice bills and the forthcoming Justice Department regulations, and refrained from completely including law enforcement and criminal justice records. However, with respect to criminal history records under the control of Federal agencies, Congress did require application of the act's general rules for public notices of record systems, for individual rights of access and challenge, and for standards governing confidentiality, security, and data quality.

A preliminary review of the hearings, documents, reports, and commentaries shows that many of the issues and questions raised in this report are not new. They have been raised and discussed ever since the CCH plan was conceived. Some of them have been discussed since the founding of our country. They have been the subject of numerous congressional hearings, of countless studies and conferences by private organizations, of judicial decisions, and of scholarly commentaries by experts. They have concerned Presidents, legislators, and judges; special interest groups in the public and private sector; public interest groups; and professional organizations of all kinds. They continue to concern directly every citizen who has been caught up in the machinery of criminal justice and whose record profile, however accurate or inaccurate, relevant or irrelevant, stale or timely, may be part of this Federal-State data system.

They concern every person whose chances for employment, professional license, and many other rights, benefits, and privileges may depend on someone searching a computerized file for information.

Ultimately, these questions and issues also concern every American who is a potential subject for some government decision on that person's arrest, detention, bail, prosecution, trial, sentencing, imprisonment, parole, rehabilitation, and employment. Finally, since they relate to matters of proper, fair, constitutional gathering, use, and disclosing of personal information about citizens, the issues raised by the application of technology for the CCH data system directly relate to the well-being of our Constitution and to the health of our society.

In addition to these individual concerns, these issues potentially involve every community that wants to use the best available means for fighting crime through effective law enforcement and swift, fair justice for offenders. They concern those who see popular control over local gov-

ernment as the most desirable instrument for democratic self-government. To others, Federal controls and sanctions for this kind of system are the best guarantees for freedom.

THE PRESENT SITUATION

The present situation involves plans for expansion of NCIC for message-switching capability including the CCH records.

In July 1973, the FBI asked Attorney General Richardson's permission to implement message-switching capability that "would allow NCIC users to take advantage of the NCIC telecommunications network to transmit and receive messages to and from other NCIC users. " The Deputy Attorney General on October 1, 1974 wrote the FBI Director "that it was deemed appropriate for the FBI to engage in limited message-switching but that any action to implement the decision must be preceded by the establishment and approval of an implementation plan." The NCIC Limited Message-Switching Implementation Plan was distributed in April 1975. Attorney General Levi did not act on it. FBI Director Kelley requested permission to terminate FBI participation in the CCH system. Action on this request was also deferred and the FBI was directed to proceed with decentralizing CCH records back to the participating States.

Members of Congress and concerned subcommittee chairmen have been informed that this effort would be based on adoption of a comprehensive "Blueprint" for a decentralized CCH program, and the Justice Department has agreed that this will be developed with the NCIC Advisory policy Board, interested Members of Congress, State CCH program officials, and State identification officials, Justice Department officials have also indicated that the FBI will not be authorized to perform message-switching until the approval by the Attorney General and Congress of whatever "Blueprint" is finally developed by CCH decentralization.

The Deputy Attorney General states: "the Department has no preconceived notion as to what ultimate solution will be adopted. " "The goals which we shall be striving toward include identifying and implementing the type of system(s) which satisfy both the spirit of our constitutional democracy and the needs of our criminal justice community. " The Department views these as "fully compatible goals. "

At the same time, the States are preparing their own positions as to the future of CCH, both individually and through their membership in SEARCH-Group, Inc.

Reasons for the FBI's lack of enthusiasm for continued participation in the CCH system were described as follows in an April 16, 1976 FBI memorandum: lack of State participation, underestimation of costs and effort which would be required to establish, collect, and maintain data for the more elaborate CCH record format; nonexistent or slowly developing State technologies; a lack of required discipline and cooperation within State criminal justice systems; and the controversy surrounding establishment of the CCH file which has been disruptive to the growth and progress of the CCH program. In addition, there have been misunderstandings regarding the reason the FBI is attempting to gain approval for limited message-switching; for instance, it is feared by some that the FBI is attempting to supplant the National Law Enforcement Telecommunications Systems, Inc. (NLETS), and that they would be in a position to monitor all law enforcement communications. The Identification Division has a criminal history record file representing 21.4 million records contributed by all 50 States and the FBI, while CCH has records contributed by 8 States and the FBI. Most States continue to rely primarily on the Division services and this diminishes motivation for taking part in the CCH program. Finally, there is uncertainty about the permanence of legislation and regulations to govern NCIC-CCH, particularly those on privacy and security.

In the course of this planning process, the Department of Justice and FBI officials have interviewed and evaluated the views of a number of State officials and CCH user groups. Excerpts from their report appear in appendix B.

If some of the issues and questions are old, what is new is this critical moment of decision for the future development of the system which is now faced by Congress, the Justice Depart-

ment, and the State and local agencies who use such information. Decisionmakers now are presented with new opportunities for application and rearrangement of the information-processing and telecommunications technology in the light of changes in our society, in our economy, in concepts of federalism, and in the public expectations of effective law enforcement work combined with effective government recordkeeping and fair use of information wherever it affects the citizen.

Changes in jurisdictions of the Judiciary Committees and in the congressional budget process mean that for the first time in the debate over the issues, responsibility for substantive policy and Legislative oversight is joined with responsibility on the FBI budget. What is new, furthermore, is increased awareness of the need for careful fact-finding on matters which may determine the successful structuring of the CCH system according to the changing and varied needs of government and society.

CHAPTER 3

Issues

NCIC/CCH ISSUES LIST

Information Needs

CRIMINAL JUSTICE REQUIREMENTS

The requirements of the Criminal Justice System for CCH information are not identified sufficiently to support planning and evaluation of an interstate system. (Seep. 17.)

CONSTITUTIONAL RIGHTS

The threats to constitutional rights potentially posed by a CCH system are not sufficiently identified for planning and evaluation of an interstate system. (See p. 20.)

Federalism

DIVISION OF AUTHORITY

What authority should be allocated among the units of government to control the contemplated CCH system in terms of efficacy, legality, and accountability? (See p. 25.)

COST APPORTIONMENT

How shall the costs of developing and operating the contemplated system be apportioned among Federal, State, and local governments? (See p. 27.)

Organization, Management, and Oversight

MANAGEMENT RESPONSIBILITIES

Considering the decentralized nature of the Criminal Justice System, what sort of management structure is required for CCH? (Seep. 29.)

OVERSIGHT

What oversight mechanisms are needed to ensure that the CCH system will operate in the overall public interest? (See p. 31.)

MANAGING AGENCY

What are the requirements for an agency to manage the CCH System? (Seep. 33.)

The Planning Process

PARTICIPATION IN PLANNING

How can the needs and interests of the various levels of government, the criminal justice community and other stakeholder groups best be accommodated in the planning and design of the contemplated system? (Seep. 35.)

TECHNICAL ALTERNATIVES

What technical alternatives to the proposed message-switching system might offer advantages when the fuIl range of system requirements and social concerns are considered? (See p. 37.)

TRANSITION PLANNING

Considering the significant change in criminal justice recordkeeping that CCH implies and the long transition period before it can be implemented fully, what aspects of this transitional period require planning now? (See p. 40.)

Social Impacts

EFFECTS ON THE CRIMINAL JUSTICE SYSTEM

In what ways, desirable, or undesirable, might CCH cause, or contribute to changes in the operation or organization of the criminal justice system? (See p. 44.)

THE DOSSIER SOCIETY

To what extent, if any, might CCH contribute to the growth of Federal social control, or become an instrument for subversion of the democratic process? (See p. 46.)

PRIVACY AND CIVIL LIBERTIES TRENDS

Is there a conflict between maintaining national privacy and civil liberties trends and decentralizing responsibility for the CCH system? (See p. 47.)

CHAPTER 3

Issues

INFORMATION NEEDS

Criminal Justice Requirements

ISSUE

The requirements of the criminal justice system for Computerized Criminal History information are not identified sufficiently to support planning and evaluation of an interstate system.

SUMMARY

Criminal justice and law enforcement practitioners are virtually unanimous in their view that interstate exchange of criminal history information is necessary for the efficient and effective administration of justice. Criminal justice agencies at all functional levels, from police to prisons, could benefit. Interstate exchange of criminal history information could aid ongoing efforts to identify career criminals, to fit decisions and treatments to the individual criminal as well as the crime, and to reduce disparities in prosecution, sentencing, commitment, and parole decisions. The benefits of rapid access to out-of-State criminal history records are suggested, but not conclusively demonstrated, by preliminary studies. As many as 30 percent of individuals with criminal history records show arrests in more than one State, and many criminal justice agencies perceive a need for immediate access to criminal histories. As the mobility of the population increases in the next decade, this demand will also increase.

Yet attainment of these promised benefits requires that criminal history records themselves be complete, accurate, and current. Moreover, the mechanism to permit interstate exchange must be designed to conformity to State and Federal restrictions on the dissemination of criminal histories. The value of out-of-State criminal history information might be limited if positive identification linking the subject with the record cannot be made promptly. The extent or problems of the identification requirement are not well established.

Much more investigation is required to assess the merits of the proposed Computerized Criminal History (CCH) System and to evaluate alternatives.

QUESTIONS

1. In what ways do, or could, the various State criminal justice agencies use CCH information to support the administration of criminal justice including criminal justice decisionmaking?
2. How do, or could, the numerous Federal law enforcement agencies make use of CCH information?
3. To what extent do in-State criminal histories satisfy the needs of State criminal justice agencies?
4. To what extent, and for what types of crimes, would access to out-of-State CCH information on a regional basis satisfy the needs of State criminal justice agencies?
5. In what ways are the requirements for nationwide access to CCH of Federal law-enforcement agencies different from the needs of State and local agencies?
6. To what extent do differences in laws and practices among States constrain or limit the value of interstate dissemination of CCH information?
7. To what extent, and in what circumstances, could CCH needs of criminal justice agencies be satisfied by system response times of 1 or 2 days or a few hours?
8. Do police users of CCH information require significantly faster response times for investigatory purposes? Why?

36-738 O - 78 - 4

To what extent is positive fingerprint identification required before using CCH information in criminal justice decision-making?

10. What will be the operational impact if identification bureaus cannot respond to indentification requests within a few hours.

DISCUSSION

The criminal justice system has operated over the years with inadequate information, lacking completeness, accuracy, and timeliness. It is only in the last 10 years that any significant progress has been made towards improving the level of criminal justice information systems.

Despite its limitations, the law enforcement-criminal justice community has recognized the great value of criminal history information, Since 1924 the Federal Bureau of Investigation (FBI) Identification Division has maintained a manual file of arrests, and dispositions when supplied, based on records submitted by local, State, and Federal law enforcement agencies. Routinely, but on a voluntary basis, these agencies send arrest records accompanied by fingerprints of the individual involved to the FBI where a search for an existing record is conducted. If found, the record is augmented with the new information; otherwise a new record is created. At present, the Division's identification records represent over 21 million individuals. When supplied with a fingerprint card, the FBI is able to search its files and determine if the individual has a prior record on file. This major service of the FBI is routinely used by law enforcement. Inquiries and responses are made by mail with a response time of about 2 weeks. In addition to the FBI files, some States have maintained their own State criminal history files.

These manual criminal history records, or rap sheets, tend to be incomplete. Since the historic relationship is between the FBI and local police departments, and not with the prosecution or courts, there has been no guarantee that dispositions following an arrest will be reported to the FBI. One internal FBI study showed that less than 50 percent of entries examined contained disposition data. Furthermore, of those records with dispositions, almost 20 percent were not posted until more than 18 months after the arrest. *

Criminal history information is used through-out the the justice system as a basis for decisioning. Police rely on criminal history information in evaluating potential suspects in cases under investigation. Prosecutors look to prior involvement with the justice system as a consideration in determining whether or not to prosecute a case. The information is used to determine whether an arrested individual should be detained, released on bail, or on his own recognizance. Corrections workers and judges have similar mandates and the Defense Bar has, through discovery procedures, obtained background on their clients from criminal history records.

Federal law enforcement agencies both contribute to and use criminal history information. In addition to the FBI itself, there are 27 Federal agencies with law enforcement authority that have access to this information, including for example, the Bureau of Alcohol, Tobacco and Fire Arms, the U.S. Department of Agriculture, the State Department Passport Office, the Internal Revenue Service, and the various branches of the military service.[2]

In the past, obtaining this information could take 2 weeks or more. This often meant that it wasn't available for use at points such as arraignment occurring early in the adjudication process. More recently, in at least some States **(e.g.,** California and New York) the magistrate before whom the subject must be brought without unnecessary delay has been required by statute to consider criminal history in making the decision whether to retain the subject in custody. The prosecution is similarly required to evaluate criminal history as part of the charging process. These uses of criminal history information require rapid access, usually within a few hours. In New York, there is a legal requirement for positive fingerprint identification before the information is used and the State has

'Disposition Systems and Procedures—Feasibility Study, Final Report, Nov. 11, 1976, Identification Section, FBI.

*Some of these late disposition postings are no doubt attributable to long adjudication times rather than reporting delays.

[2]NCIC Mailing/Telephone List, Nov. 7, 1977.

installed a facsimile network to make this possible.

Studies have shown that about 30 percent of individuals with criminal history records show arrests in more than one State. This evidence, and a desire to speed up and improve the quality of criminal history reporting have been important motivations for the development of the CCH program. Efforts have gone both in the direction of improving the data-handling and reporting procedures, including automation, within the States, and developing a nationwide CCH program to make out-of-State criminal history information rapidly available.

A better and more quantitative assessment of the situations in which out-of-State data could be useful and the rapidity with which the information is needed would greatly assist the CCH planning process. Some survey should be conducted on the state of the law concerning the requirement that prior criminal history be considered in charging, receiving evidence, and passing sentence. Also useful would be an analysis of the extent to which interstate CCH information exchange would be regional in nature. It has been estimated, for instance, that more than 90 percent of the multiple-State offender records associated with people arrested in California come from contiguous States.

If positive fingerprint identification becomes a strict requirement before CCH information can be used in criminal justice decisionmaking, the utility of rapid access to out-of-State criminal history information may depend on the speed at which the identification process can be accomplished. The potential problem lies in the case where an arrest is made in State A where the person has no prior record and the CCH system discloses a record in State B. Unless a mechanism for interstate transmission and identification of fingerprints is created that will allow positive identification in a few hours, these out-of-State CCH records will either be unusable or will be used with less than positive identification.

There is no question that access to a subject's criminal history might be appropriate beyond the area of its occurrence: the Federal and State legislatures are increasingly requiring not only that the punishment fit the crime, but the prosecution fit the criminal. And on the face of it, the criminal justice user is working with only part of potentially available information if out-of-State records are not available. But there have been no analyses performed to show the potentiaI benefit to any criminal justice decisions of the use of out-of-State data. However, surveys of potential user's perceived needs do show a general desire to have this data available.[3]

The potential benefits of the timely availability of complete and accurate criminal history information come from the potential of improving the quality of decisionmaking. The first offender who might otherwise have been detained before trial would benefit. Society would benefit from the imprisonment of the individuals with multiple out-of-State convictions who otherwise might have been put on probation. But hard information on the potential benefits of timely availability of criminaI history is lacking. The data quality needs of criminal justice decisionmaking are also not understood.

The consequences of defects in record quality such as incomplete, incorrect, or ambiguous criminal history entries on decisionmaking is simply not known. That the criminal history files presently in use are woefully incomplete seems clear. Undoubtedly a concerted effort must be undertaken to improve disposition reporting. But since no system can ever be made perfect, some level of error will always exist. Quantitative measures on data quality matters will be difficult to come by. However, the attempt is essential because of the apparent conflict between the perceived needs of the justice system and the concerns discussed in the next section that defects in record quality could lead to significant harm to individuals' rights to due process and privacy.

[3]Search Group Inc., "The American Criminal History Record, " Sacramento, Calif., Technical Report No. 14, 1976.

Constitutional Rights

ISSUE

The threats to constitutional rights potentially posed by a CCH system are not sufficiently identified for planning and evaluation of an interstate system.

SUMMARY

The CCH system was conceived to enhance the administration and effectiveness of the criminal justice system. This objective is certainly in the public interest. Also certainly in the public interest are the protection of the privacy, civil liberties, and rights to due process, of individuals affected by the system together with rights of freedom of information. Harmonizing these parallel and sometimes conflicting interests will require public policy decisions. The present climate is clouded by the absence of well-established information on the completeness, ambiguities, and accuracy of criminal history data, and on the nature of injuries to individuals that could be caused by improper use of CCH records or inadequate CCH records. The extent of actual incidence of such injuries is also unknown.

It must be recognized that computerization can eliminate certain kinds of errors that plague existing manual records. Yet, because manual records are not disseminated widely, the errors tend to be localized. With computers, the transaction volume and dissemination will increase, as will the capacity to widely disseminate inaccurate or incomplete records. The potential for harm is therefore much greater with computerized systems. It is important for policy makers to understand the origins, frequency, and consequences of erroneous or incomplete records in order to strike a fair balance between potential harm and potential benefits.

CCH information is also used for evaluation of applicants for employment or licenses as permitted by Federal and State statutes. Since State practices differ considerably, the effect of interstate CCH could be significant. The harm to individuals' employability that can be caused by incomplete, inaccurate, or improperly disclosed records is recognized, but information on the extent of the problem is not available.

There has been considerable debate on the merits of purging or sealing criminal history information based on considerations such as age of record, or the principle that such information is unlikely to provide a reliable guide to the behavior of the individual. While a few States have established such procedures, present Federal regulations set no such requirements. Again, little hard information is available to guide policy on this matter.

Another viewpoint is that criminal history information is public record material that should be made available under freedom of information principles.

Dissemination of CCH information is limited and controlled by statute in some States and by Department of Justice regulations. However, individual State planning, modification of the regulations, and demonstration of compliance has moved very slowly. The Law Enforcement Assistance Administration (LEAA) extended the deadline for submission of State dissemination plans to March 1978, an extension of 2 years from the original schedule, **an** indication of the difficulties involved. Generally, the plans submitted are expressions of intent, not of compliance actually achieved.

Further information is needed to assess the potential danger to constitutional rights, as well as the needs and benefits of CCH discussed in the previous section, before conclusions as to the proper data quality standards and dissemination restrictions can be drawn.

QUESTIONS

1. To what extent do the records submitted by the individual States and the Federal Government comply with the existing standards of accuracy, completeness, security, currency, etc., established in Title 28 CFR?
2. What sorts of injury to individuals can result from the use of incomplete or inaccurate CCH information in any category of criminal justice decisionmaking?
3. To what extent do these injuries occur?
4. What other uses of the CCH files or inquiries, such as "flagging" the names of individuals involved in activities protected

by the first amendment, for example, might present a threat to individual rights or civil liberties?

5. To what extent, if any, might the interstate dissemination of CCH information create or increase civil liberties problems in:
   a. differences among States in definition of crimes causing error or confusion in criminal justice decisionmaking based on out-of-State CCH information;
   b. Disclosure of out-of-State information to employers or others that would not be permissible in the State record?
6. What purging or sealing policy, if any, should be established to limit the "memory" of the CCH system for individuals who have had no recent arrest history?
7. Are existing access controls and logging requirements sufficient to control unauthorized use of CCH data?
8. How can the system be effectively monitored and audited to ensure that the system standards are met?
9. What monitoring and auditing mechanisms can ensure that actual occurrences of injury to individual liberties will become known to the system and to the public?
10. Which local, State, or Federal programs for handling CCH information have been most effective in protecting constitutional rights? How might other National Crime Information Center (NCIC) participants be encouraged to consider adoption of these programs?
11. What changes, if any, should be considered in standards regarding listing of arrest charges, CCH disposition entries, investigative uses of CCH records, and validation of CCH records to protect the civil rights and liberties of persons whose records are contained in the system?
12. What changes, if any, to existing Federal resolutions or laws, should be considered for protection of individual rights when CCH information is used for preemployment or licensing purposes?
13. If the privacy act is amended to cover criminal investigatory records, if Federal agencies lose their sovereign immunity protection, and/or State courts decide to remove such immunity for State governments, to what extent will there be less need for congressional action regarding NCIC privacy safeguards?

DISCUSSION

A variety of concerns have been expressed regarding the effect of the CCH program on constitutional rights. The most immediate concerns deal with the possibilities of direct harm to individuals involved in the criminal justice process through the use of CCH information to support decisionmaking. Similarly, the prospective effects on individuals of dissemination of CCH information for preemployment and licensing purposes has raised concerns. These are the main subjects discussed in this section. Less immediate civil liberties issues such as potential long-term effects of CCH on the criminal justice system, or the potential of the system to be manipulated illegally are discussed under Social Impacts (p. 44.)

CCH AND CRIMINAL JUSTICE DECISIONMAKING

Criminal history records are used by all segments of the criminal justice community for a variety of purposes. During the investigation of a crime, police may examine criminal history records of potential suspects under the belief that a prior history of arrests for crimes similar to the one in question, or the lack thereof, is suggestive of the subject's likely involvement. Criminal histories can provide useful leads to an investigator such as aliases and prior addresses.

After arrest, if available in time, criminal history records are commonly used to evaluate the defendant's right to release on bail. In many jurisdictions, criminal history records influence the district attorney's decisions as to obtaining a felony indictment, or willingness to accept a misdemeanor disposition. In some States, laws specify that prior convictions raise to the felony level a crime that otherwise would have been a misdemeanor.

After conviction, most State laws require the court to consider the defendant's criminal his-

tory record in determining the sentence. Probation officers and officials in many other programs use criminal histories to assist in their decisionmaking. Correctional officials use the information to assist in assigning the individual while he is institutionalized. Finally, parole boards in some States request criminal history records when determining whether an inmate should be released on parole.

The speed of response needed for these different uses of criminal history records varies widely. Response time measured in hours is probably adequate for most purposes. Law enforcement agencies have expressed a need for much faster response times,[4] but strong substantiating arguments have not been presented.

This pervasive use of criminal history information throughout the justice system was one of the motivating forces for development of CCH so that the information would be available in a timely manner, and to improve the tracking of events in the processing of each case so that the criminal history record would reflect the final disposition. Following the recommendations of a Presidential Commission in 1967,[5] rapid development of State computerized criminal history programs took place. According to the FBI, 20 States are now either full participants in the NCIC/CCH program or in the final stages of program development.

CRIMINAL HISTORY RECORD QUALITY

The operations of the criminal justice system impose some limitations on the quality of criminal history records. First, an offender's record is not necessarily representative of the behavior which mandated the creation of (or additions to) his record; and second, some criminal justice agencies are more cooperative and responsive than others in furnishing the data. Both of these situations affect fundamental aspects of data quality. Other important aspects would include policies on who can enter or change data, how can the data be changed, when data are to be sealed, and to what extent they are sealed from different users,

[4] 1bid.

[5] President's Commission on Law Enforcement and Administration of Justice, The Challenge of *Crime in a Free Society,* U.S. Government Printing Office, 1967.

The ability of the written record to accurately document the past criminal behavior of an offender is poor and will remain so for the foreseeable future. First, not all of the offender's known offenses result in conviction. A rule of thumb is that it takes about three arrests before a conviction is secured, because of formal and informal diversion programs. Second, even when a conviction is secured, plea bargaining often makes it unlikely that the charge at conviction reflects the nature of the criminal event. And since plea bargaining is more prevalent in urban than rural areas, this means that a rural offender committing the same offenses as an urban offender will probably look a lot worse on paper (or on CCH) than his urban counterpart. On the other hand, the charges at arrest may exaggerate the nature of the event. The police may overcharge an individual, knowing that it will probably be bargained down to a lesser charge.

Criminal history records are often incomplete. Arrests are recorded quickly, while dispositions are recorded more leisurely, if at all (in some jurisdictions). Part of the reason is the fact that the police are responsible for supplying arrest data to the FBI, while the prosecutor and courts have the disposition data and do not have as strong a relationship with the FBI as the police. Furthermore, the judiciary is a separate branch of Government, so its cooperation in a CCH system run primarily by and for enforcement agencies has been limited.

There is evidence that disposition reporting is slowly improving. Certainly the intent is clear, The LEAA regulations mandate disposition reporting within 90 days. The States are now preparing plans setting forth their operational procedures to comply with this requirement. Successful implementation of prompt and complete disposition reporting is of utmost importance to any future success of CCH systems.

RECORD QUALITY DEFICIENCIES

The implementations of CCH has brought into focus a number of concerns about criminal justice decisionmaking, most of which relate to claimed deficiencies in some aspect of record quality, e.g., accuracy, currency, or completeness. The most apparent of these deficiencies is absence of disposition information associated with arrest entries in the record. Because of delays and gaps in the reporting procedures it

has been estimated that 50 percent of the arrest records do not have disposition information. * Other alleged deficiencies include partial, erroneous, and ambiguous disposition listings.

Many of the civil liberties questions regarding CCH—in particular questions of due process—center on the effects of record deficiencies on criminal justice decisionmaking. The criminal justice process is characterized by the exercise of great discretion and bargaining at key points. Much of this discretion is exercised informally, and is in part influenced by the criminal history record of individuals, In some urban areas, more than 50 percent of those arrested by police are screened out of the judicial process before formal accusation; of those who do make a court appearance, the vast majority plead guilty in accordance with pre-arranged bargains struck between defendants, prosecutors, and police. (This topic is discussed in more detail in the Social Impacts section of this report.)

Those questioning the CCH system have argued that an individual's prior arrests count against him in the bargaining process even where the arrest charges were eventually dropped or the case resulted in an acquittal because this information is often not contained in the criminal history. The argument is made that the situation is so serious that entries without dispositions should not be permitted to be used, even by criminal justice agencies, unless the case is definitely known to be still pending. Others argue that this measure would deny highly useful information to officials who are fully competent to understand the limitations of the data, and would result in saturation of the system.

This debate is now being argued in the courts. At least one major case[6] is in process at this time arguing that the State CCH records maintained and disseminated by the New York State Division of Criminal Justice Services and supplied by the New York Police Department have poor data quality with the consequence that constitutional rights of individuals have been violated. Although the issues in this case are directed entirely at New York State's own CCH system, its outcome may have profound implications on all aspects of interstate CCH.

This whole issue is badly clouded by lack of information. We need to know the real extent of quality deficiencies in both the existing manual and computerized criminal history systems. It is unfortunate that so little assessment of data quality has taken place. Neither the State CCH repositories nor the FBI have conducted the kinds of audits that would supply this information. Nor is there much documentation other than anecdotal evidence of the extent to which individual rights are actually being affected by the present system. Also, the data is not available to estimate the relative extent of undercharging (plea bargaining, etc.) and overcharging and the conditions under which each occur.

Standards for access and security and privacy have been the subject of extensive debate. [7,8,9] But in the absence of quantitative information about the weaknesses of existing practices, and an understanding of the obstacles to their improvement, the necessary discussion of what standards should be becomes very difficult.

PREEMPLOYMENT AND LICENSING USE OF CCH

Criminal history record information is also disseminated for local and State employment or licensing purposes to the extent that it is authorized by Federal or State statutes. It is estimated [10] that 20 percent of the requests for State CCH information originate from noncriminal justice agencies. By present regulations, " arrest data more than 1 year old is not disseminated for

*The FBI, in a recent internal study (see footnote 1) found that less than 50 percent of the entries in their manual criminal history file contained disposition data. A recent sample of New York State records (see footnote 6) showed a blank disposition column in .57.3 percent of listed arrest events since Jan. 1, 1973.

[6]Taturn, et *al. vs. Rogers,* 75 Civ. 2782 (S.D.N.Y.) Plaintiff's Pre-Trial Memorandum of Law, Sept. 9, 1977.

[7]Search Group Inc., "Standards for Security and Privacy of Criminal Justice Information, " Sacramento, Calif., Technical Report No. 13 (Revised), January 1978.

[8]Search Group Inc., "Access to Criminal Justice Information, " Sacramento, Calif., Technical Memorandum No. 14, October 1977.

[9]M. D. Maltz, "Privacy, Criminal Records and Information Systems, " in Operations *Research in Law Enforcement, Justice, and Societal Security,* Lexington Books, 1976.

[10]Search Group Inc., "The American Criminal History Record. "

[11]28 CFR—-Judicial Administration, 20.33(3).

these purposes without accompanying disposition information unless active prosecution of the charge is known to be pending. Federal agencies authorized to obtain information for employment background checks under authority of Federal Executive Order receive criminal history information without restriction and generally have access to Federal investigative and intelligence information as well.

Individual States have their own regulations and statutes to govern dissemination for these purposes. The State regulations vary drastically regarding the types of employments and licensing for which criminal histories can be used.[12] Furthermore, some regulations contain procedures for deleting information not deemed relevant to these uses of the data. As a consequence of the diversity of State regulations, it is likely that information may be obtainable from another State that is not permissible for use in the inquiring State. Furthermore, information now available for Federal agency background checks through the FBI files might become unavailable if the inquiry is made directly to the State of origin. Careful control and monitoring over interstate dissemination for these purposes may thus be required to ensure that all appropriate regulations are being met.

One member of the working group felt that the private sector is entitled to more access to CCH information and that denial of this access only forces the use of illegal or roundabout approaches to obtain access.[13] For example, in Illinois, a Firearms Ownership Identification Card (FOIC) is required for an individual who wishes to own a gun legally. Grounds for denying an individual an FOIC include conviction of a criminal offense. Some firms require a prospective employee to obtain an FOIC (at the firm's expense) as a precondition of employment. In this way, they find out if the prospective employee has a criminal record. Numerous examples of illegal disclosure of criminal history information by police personnel have also been reported.

He further argues that too stringent restrictions on access by private sector employers could make matters worse, especially in light of the liberal access permitted Federal Government employers. As the law presently stands, the Department of Labor can check the record of every clerk-typist it considers hiring, but the Potomac Electric Power Company cannot determine if its prospective meter readers have records of home invasion or rape; the Social Security Administration can prevent those with criminal records from becoming janitors, but a small business cannot ensure that it is not hiring a newly released embezzler as a bookkeeper.

In this view, a better balance of access is needed and might be obtained through a less restrictive approach to the private sector's information needs.

[12] Amercian Bar Association, "Laws, Licenses, and the Offender's Right to Work," National Clearing House on Offender Employment Restrictions, 1974.

[13] M.D. Maltz]tz, "privacy, criminal Records and Information Systems," in *Operations Research in Law Enforcement, Justice, and Societal Security,* Lexington Books, 1976.

FEDERALISM

Division of Authority

ISSUE

What authority should be allocated among the units of Government to control the contemplated CCH system in terms of efficacy, legality, and accountability?

SUMMARY

Because of the decentralized nature of the U.S. criminal justice system and because the generation and use of criminal history information occurs mostly at the State and local levels of government, the States have a primary stake in establishing standards and procedures for the keeping and dissemination of criminal history information. On the other hand, minimum national standards also are required for an interstate CCH system. Attempts at comprehensive Federal legislation to control the collection and dissemination of criminal justice information have failed to produce legislation or a consensus as to how authority for this important area of control of the system should be allocated. The lack of resolution of this issue is a very serious obstacle to the successful development of CCH.

QUESTIONS

1. How should the authority for establishing dissemination constraints, and purging or sealing requirements be allocated between the Federal and State governments?
2. To what extent can control of operational procedures, including access control and employment standards be left to the discretion of the States?
3. What provisions shall be made for resolution of intergovernmental and interagency conflicts over system control?
4. How best can audit responsibilities be apportioned among levels of government, participating agencies, and representatives of the general public?
5. How should authority be divided between Federal and State governments for determination of violations and imposition of sanctions?

The extent to which interstate dissemination of CCH data presents civil liberties problems because of the diversity in State regulations is difficult to assess without more information on current practices. The questions about data quality raised regarding criminal justice uses of the data apply here as well. Since it is required that entries without disposition are not to be distributed for employment and licensing purposes, the data quality questions here focus on the clarity, accuracy, and completeness of disposition listings.

DISCUSSION

Almost every aspect of the NCIC/CCH problem encounters difficulties resulting from the historic, constitutional division of powers and duties in our Federal system. This division, while providing protection against tyranny, corruption, and other abuses, nevertheless invites conflict, error, and confusion in the **ac**complishment of valid governmental purposes. With respect to criminal justice, the foundations of the federalism issues are:

- State governments have basic jurisdiction over law enforcement and criminal justice within their borders, under their constitutionally reserved powers. Within that system, local governments play a strong role.
- Due to the mobility of both State and Federal law violators, effective law enforcement increasingly requires exchange of information among States and between States and the Federal Government.
- The Federal Government's superior taxing power and its expanded functions under the commerce clause have led to its involvement in law enforcement at local and State levels; many an intrastate crime is a Federal crime.

The sheer existence of the technical capability that can speed information across existing political-organizational barriers challenges a political structure inherited from a previous era. Organizational problems arise because a chang-

ing political environment increasingly is sensitive to the information policies of executive agencies. More traditional questions arise concerned with the sharing of costs among State and Federal levels of government, interstate relationships, and the relation between Federal and State criminal justice functions.

Given this diversity of American political and administrative culture, the CCH system is very ambitious when compared to other Federal computer systems of national scope. Compared to the Internal Revenue Service's Tax Administration System, which administers a uniform Federal tax code with personnel trained in accordance with uniform standards and criteria, the CCH system seeks to coordinate the law enforcement activities of a very diverse group of agencies, whose personnel and indeed whose laws are very different from one another.

If it is going to work, the CCH system will require data and procedures that meet prescribed minimum nationwide standards of quality and uniformity. At the same time most of the basic source records originate within local and State law enforcement agencies. State and local governments vary in their resources, their philosophies of privacy and publicity, and their sophistication in data systems technology. Decisions that are necessary to assure an effective nationwide system may conflict head-on with State laws and rules governing access to criminal justice records, the format and content of such records, and their modification or expungement. Such decisions may require State and local governments to adopt procedures inconsistent with or excess to their own operating necessities. Both levels of government could be pressured to appropriate money, install equipment, and employ personnel against their will. Court systems, despite long-standing, cherished traditions of independence, would have to conform to bureaucratic reporting requirements imposed by others. Some of these conflicts could result in litigation, which would be time-consuming and which could result in over-narrow decisions necessarily based on the issues brought to trial in specific cases.

Many of the system management problems will call for accommodations among States, between State and local governments, between Federal and State governments, among Federal agencies, and among components of the criminal justice system at all three levels. This argues for control by a representative intergovernmental consortium, which would present its own problems of management, funding, and oversight.

Further complexity is added by the need for protection of civil liberties and privacy. No governmental mechanism well-designed for such a purpose now exists, and it may be necessary to invent one.

The issue is complicated even further by the apparent need for legislative oversight. The Judiciary Committees of both Houses of Congress, among others, can logically claim such responsibility. However, their ability to oversee adequately a complex, sensitive, and detailed system may be questioned, particularly when they are compelled to turn their attention from old and continuing responsibilities to newly urgent problems.

State legislatures may also legitimately claim the right to oversee the participation of their own governments in the contemplated system. They will be concerned with costs, operational effectiveness, security, and protection of citizens' rights under their own laws.

Another aspect of control is audit. There will be a need to review the system for fiscal integrity, general effectiveness in achieving States' objectives, and quality of management. There may also need to be a detailed operational audit, using sampling techniques, of the completeness, accuracy, and currency of the data in the file and in selected transmissions. Both announced and unannounced audits may be required. Systems users should participate in the conceptual planning and review of such audits. There must also be provision for audits of costs and effectiveness.

The issue of how authority should be divided is closely related to questions of management and oversight and can directly affect the technical configuration of CCH. Those who see the responsibility for maintaining and disseminating criminal history records falling primarily with the States, for example, will argue for viewing of CCH as many different State systems with a need to exchange information. * This State-

*The SEARCH Group Inc., Board of Directors has recently adopted a position paper that articulates this viewpoint, entitled "A Framework for Constructing an Improved National Criminal History System. "

centered concept implies a minimum of Federal oversight. It also would have no compelling reason to remain affiliated with NCIC.

Some of these unresolved problems of overlapping authority in the system will be settled only by the disposition of individual conflicts as they come up. Others may be solvable by cooperative effort among the levels of government in the planning process. (See The Planning Process, p.35) The question remains, however, whether sufficient consensus on these matters exist to permit resolution at this time.

Cost Apportionment

ISSUE

How shall the costs of developing and operating the contemplated system be apportioned among Federal, State, and Iocal governments?

SUMMARY

When all of the system development, data conversion, and operating costs associated with CCH are considered, the costs to all levels of government have been estimated to amount to several hundred millions of dollars over a 10-year period. Costs of related activities, such as building capability in State identification bureaus could considerably raise the overall expenditures that will be required to achieve a fully operational CCH system.

It has been Government policy to support the development of CCH in part through the Department of Justice Comprehensive Data System Program (CDS). However, the great bulk of the anticipated expenditures are operating costs that will be incurred in the State and local criminal justice agencies. The abiIity or willingness of the States and local jurisdictions to provide these operating funds will in large part determine the actual rate at which **a** nationwide CCH system can become operational.

The issue of equity in funding is particularly knotty. Some States will perceive a high benefit from the system; others may feel that they are burdened with excessive expenses to provide information to other States and Federal agencies. Finally, some argue that the costs of complying with regulations imposed by higher levels of Government, whether State or Federal, should be subsidized.

Since funding policy will have a crucial role in the rate and success of CCH implementation, it is an issue that should be dealt with at this time.

QUESTIONS

1. What will it cost to develop a satisfactory system covering all States?
2. What are estimated annual operating costs?
3. On what basis should development and operating costs be apportioned among the three levels of Government?
4. To what extent should funding plans take into account the variation in capabilities and resources among State and local governments?
5. To what extent should Federal funding be provided to State and local agencies to cover operating expenses which these agencies feel are federally mandated?
6. What advantages, if any, would a system of user charges offer in the management of this system? What charging mechanisms might be employed?

DISCUSSION

The very modest initial conversion costs estimated in the FBI memoranda are trickles that will lead to a flood of expenditures. [14] Any local jurisdiction participating in the contemplated system will have to provide for complete, timely reporting by all components of the criminal justice system; an information system fully congruent with the State and Federal systems; and sufficient trained staff to assure reliable operations and to maintain data quality to established standards. The State agency concerned, whether it is a criminal justice planning and coordinating agency or a bureau of investigation, will also have to maintain a congruent system, including thoroughly effective data collection and follow-up procedures. To the extent States handle data and reporting matters through sub-state regional criminal justice

[14] U. S. Senate. Hearings: Criminal Justice Data Banks, Subcommittee on Constitutional Rights, Committee on the Judiciary, 1974, volume 11.

organizations, system modifications will have to be made at that level. A 1975 study[15] for LEAA concluded that the 10-year development and operating costs for CCH would be $361 million of which $241 million will be incurred in the participating States. This report also presents detailed models of the processing of CCH information and estimates transaction costs. However, the analysis assumed away a number of State costs such as development of full State identification bureau capabilities, Thus the total dollar cost will be much higher.

Criminal justice expenditures in total are met 60 percent by local governments, 27 percent by State governments, and 13 percent by the Federal Government (1975 figures). Such an intergovernmental division, however, is probably a poor guide for financing system developments, for the system improvements in the past decade are attributable in large measure to LEAA money, particularly at the local level. Typical city governments claim, usually with good evidence, to be hard-pressed financially, and incapable of financing improvements in information systems. They and their State governments will look to the Federal Government to pay the costs of the contemplated system. It can be argued on the other hand that State and local governments should pay a significant share, despite fiscal strains—if they have a stake in the game they will play better than if they do not. Yet this is a time when some fiscally troubled local governments are unwilling to put up the "match" money required to obtain some Federal grants.

Significant implementation costs for participation by all States will be incurred even if the smaller States are not forced to fully automate their criminal history records.

If the State and local governments are required to participate in financing the system the strain of finding "new money" for this purpose or of cutting back other expenses to pay for it may lead to nonparticipation or inadequate participation in the system. On the other hand, system operations could well be handicapped if it is looked at as a "big brother pays all" operation—in **a** nation where States are in many respects sovereign and where crime control is a local responsibility.

A difficult subissue which must be explored in an assessment of CCH, is how to assure equity in interstate funding in relationship to benefits received. States vary as enormously in the sophistication of their criminal justice information systems as they do in geography, population, and finances. The "have-nets" will argue that if the Federal Govrnment wants them to participate in the contemplated system it should pay the developmental costs. The "haves" will contend that a disproportionate share of Federal money should not go to States with underdeveloped systems. The States themselves have a similar problem in apportioning funds to local governments which vary greatly in systems development, as in their own resources. And again, the problem is complicated if planning and financing are accomplished through substate regional organizations.

Furthermore, States which expect great benefits from the system may be more willing to shoulder the costs than States not similarly situated. It is apparent that there are enormous regional differences in the volume of interstate criminal movements. Some States, such as California and New York are the unfortunate victims of large numbers of criminals immigrating from other States; significant numbers of criminals leave these same States to prey in other States. Yet States like Vermont, New Hampshire, and South Dakota, do not experience significant migration of criminals. Put in other words, the FBI reports large regional variations in arrest activity with 8 States accounting for 62 percent of the arrests (Director of FBI, letter dated April 16, 1976; and Hearings, S. 2008, p. 306). The FBI believes there is a high correlation between arrest activity and future use of CCH message switching.

Under a decentralized CCH system, the States that are large, automated, and characterized by transient populations would bear the largest burden of out-of-State inquiries. If out-of-State inquiry volume is significant compared to the inquiries from within the State, questions of priority of service will arise, and the costs of service to out-of-State inquiries will likely be seen as an inequitable burden by the State legislature. Pressure for Federal subsidies or interstate

---

Is Institute for Law and Social Research, "Costs and Benefits of the Comprehensive Data System Program, " Washington, D. C., June 197.5.

charges to cover these costs would be likely to develop.

It is apparent therefore that States differ in terms of perceived benefits, and will continue to differ on the distribution of costs between Federal and State levels, and among the States themselves.

Generally, it is assumed that costs will be met directly through appropriated funds—from whatever levels of government. It may be feasible and desirable, however, to impose user charges on agencies (at whatever level) seeking information through the system. Such charges could serve to relieve inequities in the system due to disproportionate demands on the various States. Charges would also provide a mechanism for limiting the volume of system traffic, as users would not see CCH information as a free good. However, the differences in ability to pay might result in less affluent agencies being discouraged from using the system.

The very process of seeking legislative approval and appropriations at possibly all three levels of government will lead to public debate over costs, effectiveness, controls, civil rights, privacy, and the entire range of issues.

ORGANIZATION, MANAGEMENT, AND OVERSIGHT

Management Responsibilities

ISSUE

Considering the decentralized nature of the criminal justice system, what sort of management structure is required for CCH?

SUMMARY

It is generally assumed that the FBI runs the NCIC/CCH system and has full responsibility for its activities. Actually the FBI's role is very limited since it must deal with the individual States as autonomous entities. The responsibility for accuracy, completeness, and currency of records lies with the States as does the responsibility for an annual audit. Both the FBI and State criminal history repositories have tended to view themselves as conduits for records provided to them by others. Thus, the chain of management responsibility is weak and ambiguous.

This loose, decentralized, assignment of responsibilities is in part a direct consequence of our decentralized criminal justice system and a persistent national concern over concentrating too much power in a Federal law enforcement agency. On the other hand, serious questions arise about accountability in such a decentralized system, that would apply no matter what agency is assigned the responsibility for system management.

This question was also addressed under Federalism. (See p. 25.)

QUESTIONS

1. What authority should be allocated among the units of government to control the CCH system?

2. To what extent would the centralization of management lead to excessive Federal control over State and local criminal justice activities?

3, What would be the advantages of separating CCH from the NCIC system?

4. Is there a need to designate a single agency to have overall responsibility for the administration of the CCH system? If so, what responsibilities should be assigned to the agency responsible for managing the CCH system to ensure and validate CCH data quality?

   a. What responsibility should be placed on the system management agency to ensure that data disseminated through the CCH system is used properly?

   b. What responsibility should be placed on the system management agency to report to Congress and the public on the "health" of the system?

36-738 0 -78 - 5

c. What authority for audit and monitoring of data submitted by the States and Federal user agencies is required to satisfy these responsibilities?

d. What sanctions should be provided for violations of standards or procedures?

e. What appeal mechanism should be established?

f. What would be the merits of restructuring the Advisory Board for CCH to include representation of noncriminal justice public interest groups?

g. What new Federal legislation, if any, would be required to provide authority for the system management agency?

DISCUSSION

DECENTRALIZATION OF MANAGEMENT

The responsibility for interstate CCH dissemination is distributed rather widely at present. The FBI runs the NCIC central facility and is responsible for the NCIC procedures governing access to the system. The LEAA has established regulations on collection, storage, and dissemination of criminal history information that apply to all criminal justice agencies receiving LEAA funds directly or indirectly—covering essentially all participants in NCIC/CCH. These regulations in turn call on the **States** to submit a Criminal History Record Information Plan setting forth each State's CCH operational procedures. As of the latest revision of the regulations, these State plans must be submitted by March 1978. The regulations are explicit in allowing a wide variation among States in their dissemination policies including freedom to limit dissemination of both conviction and nonconviction information as each State sees fit.

The existing Federal law and regulations also place the responsibility for annual audit of the operation of every State's system with each State and limit the Federal involvement primarily to approval or disapproval of each State's plan. On the other hand, considerable concern about the need for congressional oversight and Federal supervision of the system has been expressed in Congress in numerous hearings[16] [17] on the subject of criminal justice information, resulting in a number of bills attempting to establish Federal standards and procedures to control collection and dissemination of such information, as well as providing for Federal audit authority.

The Federal Government's role in the day-to-day management of the NCIC/CCH system is therefore somewhat ambiguous, and neither the FBI nor the States are sure what their responsibilities are. The management solution to this dilemma may require imagination and new forms of Federal/State cooperation.

ROLE OF AN ADVISORY BOARD

The primary operational link between the FBI function as NCIC system manager and the State participants is through the NCIC Advisory Policy Board. The decentralized nature of the system's regulations argues for a strong accountability of the central operation to the users of the system. Yet the historical experience with the use of advisory boards as the formal liaison between system users and the system executive suggest that this arrangement provides for only weak accountability. [18]

Typically, members of the advisory board are not familiar with the operational intricacies of the computer system, and often are not familiar with the day-to-day system failures which become apparent to lower level, ultimate end-users. Typically, the advisory board meets infrequently; its members are only engaged part-time in monitoring the system's activities. Moreover, the operational staff of the computer system is responsible to the executive director, not the advisory board. Therefore, advisory boards have little knowledge or authority with respect to operation of the system.

16U.S. Senate, Hearings: Subcommittee on Constitutional Rights, Committee on the Judiciary, S. **2542,** S. 2810, S. 2963, and S. 2964, March 5, 1974. 93rd Congress, 2d session.

"U.S. Senate, Hearings: Subcommittee on Constitutional Rights, Committee on the Judiciary, S. 2008, S. 1427, and S. 1428. July 15 and 16, 1975. 94th Congress, 1st session. "Criminal Justice Information and Protection of Privacy Act of 1975. "

"Kenneth C. Laudon, Computer-s and **Bureaucratic** *Reform, New* York: Wiley, 1974.

For all of these reasons the advisory board method of attaining accountability to users is structurally weak. Instead of representing ultimate users to an executive, they are just as likely to function in reverse to represent and explain executive policy to lower level users.

A second issue of accountability raised by the existing NCIC Advisory Policy Board concerns the question of defining users: who are users and how shall they be defined? The current arrangement recognizes users as those directly involved in the creation of the data base and who ultimately use the data base. This confines the definition of users to the criminal justice community, and within that community, it is largely law enforcement agencies who are represented on the Advisory Policy Board. The historical insistence on law enforcement agencies for complete control over their information processes is reflected in the existing definition of user.

But CCH is not primarily for law enforcement users. Whether or not CCH continues to be part of NCIC, some means of strengthening the advisory role of the rest of the criminal justice system for CCH is needed. Furthermore, additional participation may also be desirable. Several local criminal justice agencies (Alameda County, California's CORPUS System, for example) have appointed citizens not employed by criminal justice agencies to their advisory boards. Their experience has been that inclusion of such groups is initially uncomfortable, in that issues that might otherwise be avoided in **a** club-like atmosphere of like-minded individuals are forced onto the board's agenda. But, on the other hand, generally acceptable solutions have been found that have stood the test of the inevitable public scrutiny.

Thus, it may be fruitful to examine alternatives to the present advisory board. At the opposite extreme would be an independent Executive Policy Board with substantial authority over policy decisions and ultimate responsibility for system operations. There are many alternatives between the extremes which might be explored in a future assessment.

Oversight

ISSUE

What oversight mechanisms are needed to ensure that the CCH system will operate in the overall public interest?

SUMMARY

The history of computer systems parallels that of other institutions; they routinely fail to record and analyze their failures. In large systems it is difficult to assign responsibility for system shortcomings. Exercising effective oversight over such a system challenges the intellect of experts and the patience of ordinary citizens.

The purpose of oversight is first, to assure political executives, managers, Congress, courts, and the public that the system is operating within boundaries defined by Congress. Second, oversight mechanisms can alert Congress and the public to system problems which emerge in the course of operation.

Oversight is closely linked to system audit since audit is one of the strong mechanisms available for disclosing system problems. The present NCIC regulations do not provide for Federal audit of NCIC operation. Beyond Privacy Act reporting requirements for system uses and new systems involving personal records, no public disclosure of system operations is mandated. Therefore, it is difficult to believe that there is adequate information available for effective executive branch, congressional, press, or public oversight\ of the system's activities. Justice Department and FBI officials, however, believe this problem is met by public relations activities for purposes of educating the public through speeches, lectures, films, and invited public observance of meetings of the NCIC Advisory Policy Board.

Among the mechanisms which could provide Congress with additional information by which to judge system operation are mandated management reports on system operations and ran-

dom audits of CCH files and transactions by an external group of auditors, such as the GAO. However, additional legislative authority may be required to provide for audit and access to records held by State or regional criminal history repositories.

QUESTIONS

1. What provisions should be made for legislative oversight, apart from normal Federal and State appropriation processes?
2. Is establishment of a special legislative watchdog agency for this purpose justifiable?
3. What monitoring and reporting procedures regarding system operation and audits are required to allow effective congressional or public oversight?
4. What audit mechanisms should be established for the system?
5. What further legislative authority, if any, is required to support audit requirements?

DISCUSSION

The history of computer systems parallels that of other institutions; they routinely fail to record and analyze their failures. A survey[19] of the American Federation of Information Processing Societies conducted in 1971 found that 34 percent of the American adult public had problems in the recent past with a computer. Most of the problems related to computer billing errors. Yet a visit to any of the major credit card companies in the United States and Canada would find none had ever analyzed why the errors occur.[20] The attitude is widespread that errors simply don't occur, if they do occur, they are too insignificant and random in character to worry about. Errors are commonly attributed to "human problems, " not system design. Rarely is it publicly recognized that system errors are frequent, and that they are systematic, related to system design and corporate cost-decisions of senior management.

In large systems it is increasingly difficult to find individuals responsible for system errors. Exercising effective oversight over such systems challenges the intellect of experts and the patience of ordinary citizens victimized by poor systems.

The present FBI message-switching plan[21] does not clearly specify oversight mechanisms. The purpose of such oversight: 1.) to assure Congress and the public that the proposed system is operating within boundaries defined by Congress; and 2.) to alert Congress and the public to system problems which emerge in the course of operation.

The FBI plan suggests two internal audit mechanisms. One is an internal audit team "which will travel to the States to work with State representatives to ensure that the State is complying with established rules and procedures." Secondly, routine reports are mailed to each State of CCH records deleted from the CCH file by the FBI which, presumably, States can check against their own records and inform the FBI of errors. The proposed internal audits do not authorize public disclosure of system activity or system errors and difficulties. Therefore, it is difficult to believe these internal audits would allow effective congressional or public oversight of the system's activities.

Assessment of the NCIC/CCH plan should consider if the proposed internal audit mechanisms are sufficient to permit effective oversight of the system's operation by Congress and/or the public. The assessment should consider alternative audit mechanisms which may provide Congress with additional information to judge system operation. Two approaches seem possible here.

First, a management report on system operation with specific categories of information specified in advance by Congress. Such a report would, of course, include tallies of routine system activity, e.g., numbers of cases on file, participation levels of States (inquiries and submissions), etc. More important, the report should account for system irregularities, errors, and abuses. A report of legal actions against the FBI

---

[19] American Federation of Information Processing Societies, *A National Survey of the Public's Attitudes Towards Computers*, Montvale, N. J., 1971.

[20] Theodore Sterling and Kenneth C. Laudon, "Humanizing Information Systems, " *Datamation Magazine*, December 1976.

[21] U.S. Senate. Hearings Criminal Justice Data Banks, Subcommittee on Constitutional Rights, Committee on the Judiciary, 1974, **volume** II. p. 992.

or State CCH repositories involving the NCIC/CCH file, an account of internal audit results concerned with data quality, confidentiality and security. The question of data accuracy seems especially important here. In light of the FBI approach to the CCH records, that, basically, it has custody of State records, it appears that, for puposes of auditing, the FBI would in practice construe "accuracy" **as** the degree to which FBI and State computer files agree. * But equally, if not more important, is the extent to which CCH files agree with local police arrest and court disposition data.

A second possible congressional oversight measure is a random audit of both NCIC/CCH and State CCH files by an external group of auditors such as the General Accounting Office (GAO). Banks are routinely required to file such reports, and in certain circumstances are subject to Federal audits on demand. If criminal records are thought to be as important as bank records, if the potential for abuse is large, then such a Federal audit is in order.

However, Federal legislation may be necessary to provide the GAO with adequate authority to carry such an audit. In a letter[22] to the Senate Subcommittee on Constitutional Rights, Committee on the Judiciary. The Comptroller General advised:

> we believe explicit access to the necessary criminal history data should be provided to our office in this legislation because of the sensitive nature of the data involved. We also need access to the records of all non-Federal criminal justice information systems subject to the legislation for the purpose of evaluating the Attorney General's or the Federal Information Systems Board's operations under the legislation. An explicit statement of congressional intent regarding this matter should preclude future executive agency reluctance to allow us access to documents we believe we must review to properly discharge our responsibilities. "

*According to the FBI, for their purposes, "the accuracy of a CCH record is based upon the original source document, i.e., the fingerprint card submitted by the arresting agency, conviciton data submitted by the courts and confinement data submitted by the corrections facility. The source document is the basis upon which the CCH record is prepared and submitted and remains in the custody of the original agency for ultimate verification if required. "

[22]Federal Bureau of Investigation, "National Crime Information Center—Proposed Limited Message-Switching Implementation Plan, " April 14, 1975 (Revised).

Managing Agency

ISSUE

What are the requirements for an agency to manage the CCH System?

SYSTEM

By some standards, the FBI is uniquely qualified to run the CCH program; they have the advantage of the cooperation and respect of law enforcement agencies throughout the country; they have an extensive fingerprint identification function which is necessary to support effective use of CCH where identity is in question; and the transfer of CCH to some other Government agency might be viewed with some concern by the law enforcement community. By other standards, and in light of changing public attitudes towards privacy, civil liberties, and governmental controls, the FBI is placed in a position of great conflict of interest in bearing these records management responsibilities in addition to its primary investigatory responsibilities and its responsibilities for other noncriminal records. An argument can be made that higher public confidence would be attained by placing CCH operations in a more neutral agency.

The responsiveness of FBI management to the needs and priorities of the State and local criminal justice agencies is also in question. Some feel that NCIC is at a disadvantage since it must compete for priority with internal FBI data processing applications because it is run, by and large, as an internal FBI operation. The NCIC Advisory Policy Board is supposed to provide guidance to the FBI Director on the relationships of NCIC with local and State systems. It has been suggested that the Board could carry out those functions better if it were given a more direct role in setting system priorities and direction.

QUESTIONS

1. To what extent, if any, do the FBI's responsibilities as an investigatory agency conflict with its responsibilities for the maintenance of noncriminal files, records of criminal history, and the production of criminal statistics?

2. To what extent, if any, would separation of these functions into relatively autonomous organizations reduce the potential for abuse of power?
3. Does the investigatory nature of the FBI inhibit individuals in the exercise of their rights to examine and challenge information in their files?
4. To what extent, if any, does the FBI's extensive identification capability argue for keeping CCH organizationally within the FBI?
5. To what extent, if any, does the respect and cooperation afforded the FBI by law enforcement agencies throughout the country give them important advantages as CCH system manager?
6. When all of NCIC is considered, what additional advantages of FBI operation come forth?
7. Could the FBI's management of CCH be more responsive to the user community?
8. Is NCIC in conflict with internal FBI data processing requirements with regard to priority and budget to the disadvantage of NCIC users?
9. Is there a need to increase the authority of the NCIC Advisory Policy Board to make it independent of the FBI?
10. What advantages and disadvantages would be associated with placing management responsibility for CCH in: another part of the Department of Justice; a congressional board or corporation; or an entity established by a consortium of States. What other organizational options are feasible?

DISCUSSION

Currently the NCIC (which includes eight other files besides CCH) is organizationally located within the FBI and operates much as a division of the FBI whose director is responsible to the Director of the FBI. There is an Advisory Policy Board composed of 26 members, 20 of whom are representatives of local, State, and regional users, and the other 6 members are appointed by the FBI. The Advisory Policy Board reports directly to the Director of the FBI.

The historical experience in the United States is that law enforcement agencies demand control over their investigative and other information handling procedures. Unlike other agencies at State and local levels, such as welfare, health, employment, and other information gathering State agencies, police, and to a lessor extent the other criminal justice agencies, have vigorously guarded against the intrusion of civilian oversight, handling, or control over law enforcement information. During the early computer years, and continuing to the present, this demand for near complete autonomy and total control has meant computer operators, even programmers, were required to be employees of law enforcement agencies. The demand for autonomy and control by law enforcement agencies in the handling of criminal information was generated in part by their desire to ensure the timely availability of the information. But it has also reflected a broader societal concern that said, in effect, only the police would be trusted with this information.

There are a number of reasons why both public opinion and the opinion of experts have begun to challenge the notion that law enforcement agencies (particularly the FBI) should be solely entrusted with the responsibility of gathering, storing, and retrieving criminal information. There has been (and likely will continue to be) a change in the political environment: recent history suggests that the FBI and other law enforcement agencies have used information systems (both manual and automated) for the pursuit of political goals.

The changing political environment has caused many to wonder if there can be sufficient public acceptance of the FBI's role as developer and manager of a national message-switching capability for criminal histories. If, as the FBI proposed, the CCH message-switching capability is added onto the current FBI-NCIC operation, what will prevent future misuse of the system? How will Congress exercise control and oversight, and how can such a system be made accountable to both Congress and the public?

These concerns, which essentially involve questions of political trust, are relevant to organizational issues because some ways of organizing the proposed message-switching capability may be efficacious from the point of

view of control, oversight, and accountability, than other forms of organization.

A second set of concerns argues for serious consideration of the organizational location question. It has been argued that the FBI is burdened with too many contradictory—or at least conflicting—responsibilities. The 'FBI is an investigatory agency which also bears a heavy responsibility for the maintenance of criminal records, stolen property records, and the production of criminal statistics. It is also involved in a number of programs involving training of State police officials, maintenance of an extensive forensic laboratory, and significant local aid programs.

A widely respected principle of organization suggests that unique functions (like investigation as opposed to criminal statistics) be embedded in specialized and relatively autonomous social units. Separation of the CCH system from FBI management would have serious implications without doubt. Firstly, there are the operational problems that may be incurred by organizational separation of CCH from the fingerprint identification services of the FBI. Close technical coordination with the rest of NCIC would have to be maintained to prevent awkward and expensive interface problems for the users (unless all of NCIC were moved to other management). The benefits of the FBI's Iong involvement and rapport with local law enforcement agencies would be lost. Perhaps most important, the implied criticism and official endorsement of various group's suspicions of the FBI might have very high political costs. Nevertheless, because of the fundamental issues discussed above, other management structures should be examined.

The alternatives considered need not be limited on the basis that NCIC requires law enforcement management. If the system is regarded as a utility to the criminal justice system and the communities which it serves, the alternatives of control might be considerably greater. Some readily apparent alternatives are: the criminal information function might be continued as a responsibility of the FBI; it could be separated entirely from the FBI and organized as an autonomous division within the Department of Justice; it might be organized as a congressional board or corporation; and finally it could be developed as a consortium of States.

The relevant criteria on which to judge these or other organizational alternatives would include the following: degree and likelihood of effective accountability, oversight, and responsiveness of the criminal justice information process; convenience of funding; and appropriate division of authority between States and the Federal Government.

THE PLANNING PROCESS

Participation in Planning

ISSUE

How can the needs and interests of the various levels of Government, the law enforcement-criminal justice community and other stakeholder groups best be accommodated in the planning and design of the contemplated system?

SUMMARY

The Justice Department is now in the process of developing a blueprint for CCH. It is anticipated that this blueprint will present a new proposal for decentralized CCH, and will include a plan for telecommunication,

However, the essence of the CCH system is that the primary sources and users of the data are the State and local law enforcement and criminal justice agencies. The history of CCH development has shown the importance of the States' participation in the planning process. It is questionable that a blueprint for a workable system can be created without their playing a direct, perhaps even principal role in the planning. This should be through a process which includes and integrates the views of a broad cross-section of interest groups and categories of citizens and decisionmakers in Government and

elsewhere in society who will likely be affected by the future development and use of the CCH system and related information systems.

The nature of the information in the CCH system has raised public concern and debate about privacy and due process. Special interest groups and others have had the opportunity to express their views at several congressional hearings. But there has not been any mechanism for involving these groups in the planning process. Such involvement may be necessary to the development of a workable system,

Also to be considered in the planning process should be the public at large. It would be valuable to disseminate information on the proposed CCH system and to assess the views of the public through various forms of citizen participation.

QUESTION

1. To what extent should the Federal Government dominate the CCH planning process?
2. How can rich States and municipalities, poor States and municipalities, and advanced and backward criminal justice systems be properly represented in the planning and design process?
3. Has there been any citizen or public interest group participation in the development of CCH?
4. What participation by citizens or public interest groups might be appropriate in future CCH planning?
5. What mechanisms for informing the publi about CCH and obtaining participation in planning might be appropriate in the future?

DISCUSSION

Two major themes have reappeared throughout this report. Firstly, the State and local agencies of the criminal justice system; police, courts, prosecution, and corrections, are the primary users of criminal history information in the system. They are also the basic source of the data entries that make up these records. Furthermore, the serious problems of data quality plaguing criminal justice recordkeeping can be solved only by the efforts by these agencies. The second theme has been that the CCH system cannot be considered the exclusive province of the criminal justice community. The general public has a direct interest in it because of the very nature of the data and its use in decisionmaking for criminal justice, employment, licensing, and other noncriminal justice purposes both public and private, as well as the access afforded to the press in varying degrees by the various States.

At the Federal level, there are three additional stakeholders. The FBI, as operator of NCIC/CCH, has a clear interest. The LEAA, with its major Comprehensive Data Systems Program for stimulating and funding the development of a State and local information system infrastructure, and its responsibilities for promulgating and ensuring compliance with regulations for criminal justice information systems is an additional stakeholder. In addition to these two components of the Department of Justice, there are the numerous Federal agencies with law enforcement powers who have an interest in the system as users.

With all of these diverse stakeholders, it should be obvious that the type of process employed for system planning, system modifications, and decisionmaking can have a very significant impact on the acceptance of the system, on the speed and smoothness of its implementation, and on its ultimate viability.

At the present time, the primary mechanism for system planning is the "blueprint" activity in the Department of Justice. This effort is being conducted by Justice and FBI staff, although it has had the benefit of visits to numerous State and local user agencies. * However, any plan, no matter how well founded, is bound to have controversial elements. Therefore, some thought should be given now as to the extent to which other stakeholders should be included as principals in this planning process and as to the nature and extent of a ratification process among the stakeholders will be required.

The question of participation by stakeholders arise from another consideration as well. As discussed under the section on Transition Planning

● See appendix B for a summary prepared by the Justice Department of the viewpoints expressed by State officials during these visits.

(see p. 40.), there will be a long transition path between today's criminal records system and an eventual smoothly functioning CCH system. Numerous pitfalls are inevitable along this path and modifications in system operation, procedures, and design, perhaps large ones, are inevitable. There appears to be a need therefore to have a continuing planning process rather than a one shot "blueprint." The nature of this process, and its relationship to the operation of the system also needs further examination.

Technical Alternatives

ISSUE

What technical alternatives to the proposed message-switching system might offer advantages when the full range of system requirements and social concerns are considered?

SUMMARY

The need for message traffic between States is inherent in any system based on decentralized CCH files. The proposed FBI message switching would provide telecommunications for this message traffic in a manner that would route all traffic through a "hub" under control of the FBI. This approach would integrate the CCH traffic into the existing NCIC communications network and would provide the service at no charge to the States. However, the message-switching concept has raised a furor, in part because of concern that the resulting CCH system would be equivalent to a national data bank even though the files are physically decentralized, and that control of the message switch would give the FBI excessive control over the user agencies.

Alternative approaches to managing message traffic are available that might relieve some of these concerns, while raising questions of their own. Grouping of States for CCH exchange into a number of regional networks rather than one national network may also have some advantages that should be explored.

The need for positive identification of individuals before criminal history records can be applied with confidence to criminal justice decisionmaking has been discussed since the early days of project SEARCH. At least one State, New York, requires positive fingerprint identification and has set up an intra-state facsimile network to facilitate identification within 3 hours. Projection of this requirement nationwide could lead to extensive additional telecommunications requirements. New technology offers some promise, and needs further exploration.

QUESTIONS

1. To what extent could the message-switching system be designed to prevent or detect illicit monitoring of CCH message traffic by the message switch operating agency?

2. To what extent might the system be vulnerable to monitoring or tampering with CCH files by unauthorized persons; requiring additional physical and data security measures?

3. What are the advantages and disadvantages in cost, operational characteristics, and auditability of a multinode distributed data network which would not require all messages to be routed through Washington?

4. What advantages and disadvantages, if any, would regional systems have with regard to economy, ease of management, responsiveness to local needs, protection of privacy and accountability and resolution of conflicts between units of Government?

5. Might a regional configuration obviate the need for a national pointer index by permitting economical broadcast inquiry to the regional systems?

6. If some smaller States chose to remain with manual criminal history records, would regional or national computerized pointer to these records adequately serve the needs of the other States?

7. How soon would the fingerprint and facsimile technologies be available for criminal justice use in a cost-effective manner to satisfy the identification requirements accompanying CCH?

8. What are the likely changes in cost of these technologies with time?

36-7380-78 -6

9. **What will be the effect of these technologies on the optimum national fingerprint system with regard to centralization or decentralization?**

10. **What consideration, if any, should Present** CCH system **planners give to these technologies?**

DISCUSSION

There is no doubt that present technology in data processing and communications is adequate to meet **NCIC system performance requirements. Furthermore, over the past** 10 **years, the cost of data processing technology has** been decreasing continuously. In particular, the technology associated with digital communications has undergone major changes which make the concept of distributed data processing more realizable from a cost point of view.

However, it is not so clear that present technology and system design and development tools and techniques are able to ensure adequate controls and protection to ensure the confidentiality of the information as it passes through the system, is stored on tapes and discs for rapid access, or is archived for historical purposes.

At this time, when the alternatives for implementation of CCH are being re-examined, some time should be given to looking at the possibility that newer technology could provide a more effective means of meeting the systems requirements or relieve some of the serious problems of social concern about the system.

MESSAGE SWITCHING

Message traffic between NCIC user agencies is a fundamental aspect of the system. In addition to routine administrative traffic, there are two important sources of operational message traffic between NCIC user agencies. The first is concerned with validation of NCIC "hits. " For example, if a routine NCIC inquiry about a person reveals that the NCIC wanted person file lists him as the subject of an arrest warrant held by the Chicago Police Department, the inquiring agency must contact the Chicago PD directly to determine if the warrant is still valid before it can take action. Rapid and direct communications for this purpose is obviously necessary and can minimize the likelihood of a stale or inaccurate record leading to an improper action on the part of the recipient agency. A second source of message traffic between user agencies is associated with any concept of decentralized CCH, in which criminal histories on file in one State must be communicated in response to inquiry from another State. These messages are presently handled either on the National Law Enforcement Telecommunications System (NLETS), by mail, or by direct telephone communication.

The FBI's proposed Limited Message-Switching Plan would provide for transmission of these types of messages over the NCIC telecommunications network in addition to the current traffic of messages transmitted to and from the NCIC files. The term "message switching" refers to the routing of messages between user criminal justice agencies by means of the NCIC communications network and its central computer. The communications network can be viewed as a wheel with the FBI computer as the hub and the communications lines leading to each of the States as spokes. Transmission of data messages between agencies over this network therefore requires transmission from the inquiring agency to the hub and then retransmission to the addressed agency. Replies would operate the same way. Use of the NCIC communications network in this fashion could be a rapid and economical way of managing the system's message traffic.

Although the message-switching approach to data communications is becoming quite common, it has encountered potent opposition when applied to the NCIC situation. One primary reason for this opposition is concern that the FBI, in managing the message switch, would obtain excessive control over the user agencies and an opportunity to monitor the traffic for political purposes. This opposition is also fed by a fear that message switching would provide the capability of integrating CCH data held by the States for purposes not intended for the system and that consequently CCH could become an uncontrollable national data bank. In this respect message switching for NCIC has become associated with more 'generalized concerns about the creation and abuse of national data banks in our society.

The choice of technological configurations for the CCH system can have a very strong interaction with the organizational and social architecture of the system. The centrally controlled features of the proposed message-switching plan are inextricably linked with the organizational assumption that the system is to be operated by the FBI and funded by the Federal Government.

Other technical approaches to managing message traffic between users may be feasible that would not require traffic between States to be routed through a central hub, with its overtones of Federal control. At the same time, such a configuration would be likely to place more responsibility on the States for traffic logging and for identifying and correcting errors in the CCH index. Also, removal of the Washington hub for message traffic would tend to focus oversight attention towards the States.

With all of these interactions as well as considerations of security and economy in mind, alternative technical approaches to message switching should be explored.

ALTERNATIVE SYSTEMS CONFIGURATIONS

Three general configurations for a "national" CCH system can be contemplated. On one extreme is the centralized data base; on the other, the completely decentralized system in which record segments, identified from a central index, are collected from the various States and assembled at the site of the inquirer. In the middle is the 1975 FBI proposal of State-held records on single-State offenders and centralized records on multi-State and Federal offenders, all controlled through a centralized index.

The centralized data base concept is the one presently in operation. Its deficiencies are well demonstrated. It requires complete duplication of records at the central location and a means of maintaining their currency in addition to the maintenance of the State files. The States lose operational control of the dissemination of their data. For both political and economic reasons, many States have not joined the national system.

The completely decentralized system would leave all criminal history records in State repositories with only Federal offender records and a pointer index at the national level. Local criminal justice officials argue that the State is best qualified to interpret information on offenses occurring within the State, and consequently it is the most appropriate and effective repository for such records. Furthermore, decentralization would retain for the States much more effective control over the dissemination of records than is possible with a centralized system.

On the other hand, the fully decentralized system with centralized message switching would have the maximum amount of, and expense for, message traffic of all alternatives.

The middle ground involving centralization of multi-State offender records has the potential advantage of reducing the amount of message traffic as compared to the fully decentralized concept. However, it also partakes of the disadvantages of the fully centralized system discussed above.

A concept of regional sharing of information, with regional criminal history repositories interconnected in a national system, appears to have few, if any, advocates at the present time. However, if criminal activity has a regional character, as the fragmentary data available suggests, then suitably chosen regional repositories would find that most inquiries are intraregional. Most inquiries to the national pointer index would indicate no out-of-region record, and national message traffic could be significantly reduced. Existence of regional repositories might also benefit smaller States that otherwise would be reluctant to computerize their own records.

The political, organizational, administrative, and economic dimensions of regionalization have not been explored, however.

Considering the interplay already discussed between the technological, political, organizational, and social architectures of this system, detailed examination of these alternatives should be explored further before a choice is made.

IDENTIFICATION TECHNOLOGY

Identification technology is an area in which future technology developments could make a significant difference. As discussed previously in this report, one of the weaknesses of the CCH system as currently conceived is that rapid identification by fingerprints is not available on a

routine basis. The two bottlenecks to achieving this are the time-consuming and expensive process of manual technical search of fingerprint files, and the present high cost of facsimile transmission of fingerprints.

Technology offers the prospect of solving both of these problems. The FBI has invested heavily in the past 10 years in the development of the FINDER system for fingerprint encoding and search. This system, now being installed in the FBI Identification Division, is almost completely automated. Total equipment and software costs until completion have been estimated at $57.2 million. In addition, the training and skills required to operate the system are extensive. Nevertheless, a highly automated fingerprint identification system is on the verge of being demonstrated to be economical, at least for the FBI's very large collection. More recently the Canadian Government has ordered a similar system to be installed at the RCMP headquarters in Ottawa. This system, with a file of 2 million fingerprint records is about the size that would be required by a State identification bureau. The problem of economical fingerprint transmission still remains. But here too, recent developments in digital facsimile systems, including some technology developed with LEAA support, shows promise of leading to practical and economical hardware.

It is not clear without further study how soon these technologies are likely to be available and economical enough for widespread use. Furthermore, depending on the relative costs of the FINDER and facsimile technologies, they could have the effect of encouraging either centralization or decentralization of the Nation's fingerprint identification activities.

Transition Planning

ISSUE

Considering the significant change in criminal justice recordkeeping that CCH implies and the long transition period before it can be implemented fully, what aspects of this transitional period require planning now?

SUMMARY

Much discussion of CCH tends either to criticize problems and imbalances of today's system environment or to focus on design of an ultimate system operating at some time in the future. It is tacitly assumed that a transition path between the two can be found. However, explicit planning will be necessary to avoid dangerous pitfalls along this path.

The gradual conversion from manual to automated criminal justice recordkeeping is accomplishing a steady improvement in both the accuracy and completeness of records. At the same time, more extensive use of the records has been made possible. There is good reason to question whether the quality of today's records is adequate to support the uses to which they are beginning to be put in criminal justice decisionmaking. System planning should recognize that there will be an extended period in which most criminal history records do not meet standards of quality. Interim procedures and monitoring may be desirable, as is coordination of the pace of implementation of improved intrastate information systems with the rate of interstate CCH implementation.

A large number of cost-related questions not currently addressed by the FBI need to be addressed. The rate of development of State systems needed to support CCH is in large part determined by Department of Justice policies and funding which affect systems development primarily. Yet the States have concerns about the operating cost impact of the new systems and may resist Federal requirements, such as audit, that could add to their operating costs.

Also related to CCH planning is the relationship between the FBI's Identification Division, the State Identification Bureaus and CCH. For the next 5 years or more, until CCH is substantially operational, the manual rap sheet activities of the Identification Division will have to be continued. In the long run, maintenance of the two systems will obviously be duplicative. There is no FBI plan dealing with this question.

Finally, there are some questions about poor response time in the existing NCIC system. FBI statistics made available to the working group

support the inference that long delays in system response have been caused by system outages resulting from both hardware and software failures. while a long-term solution to these problems should be addressed as part of the overall planning process, it will be 3 to 4 years, if not longer, before longer term plans can have effect.

It will be highly desirable if all of these transition questions are addressed in the blueprint for NCIC/CCH now being developed by the Justice Department.

QUESTIONS

1. What planning exists or will be developed in the CCH blueprint for ensuring the improvement of CCH data quality and adequately minimizing the effects of poor data quality?
2. What is the proper balance of emphasis between building intrastate CCH capability and stimulating interstate dissemination?
3. Are special audit procedures required to monitor the social risks of CCH during the early years of operation?
4. How will the CCH blueprint plan to incorporate States that choose not to computerize their criminal history records?
5. Will the CCH blueprint include cost estimates and a financing plan for the system?
6. What will be the short- and long-term relationship between the FBI Identification Division and the CCH program?
7. What is the relevance, if any, to dissemination of criminal history information from the Identification Division files of questions that have been raised regarding CCH dissemination?
8. What would be the advantages and disadvantages of integrating CCH and Identification Division record formats?
9. What would be the advantages and disadvantages of making CCH an integral part of the Identification Division data base?
10. What would be the advantages and disadvantages of allowing State Identification Bureaus to have remote online **access to** the Automated Identification Division System (AIDS)?

DISCUSSION

The Justice Department is now in the process of developing a blueprint for CCH. It is anticipated that this blueprint will present a new proposal for decentralized CCH, and will include a plan for the necessary telecommunications.

Because of the significant change in criminal justice recordkeeping that CCH implies, and the long transition period that will be required before the system can be fully implemented, it is crucial that the CCH blueprint should lay out a plan dealing explicitly with how the transition will be managed.

The following pages deal with several transition issues: the problem of poor data quality during the transition period; the problem of managing a mix of manual and computerized record systems in different States; the issue of system costs and financing; the relationship between the CCH program and the FBI Identification Division; and finally, the issue of response-time problems in the existing systems.

TRANSITION FROM MANUAL TO COMPUTERIZED RECORDS

In the typical system with a large data base, the transition from manual records to computer-based records is a period in which many errors and gaps in the manual records are systematically uncovered. System managements differ in the treatment of deficient records: the files may be expunged entirely, they may be flagged but entered in the system, or they may be reconstructed and then entered. Each strategy presents certain costs and benefits to management. The transition to computerized records offers management the opportunity to significantly increase the quality of the data base. This process is occurring as States and local agencies convert their criminal history records to computerized form. The quality of criminal history records is certainly being improved. The problem of poor disposition reporting, for example, was far worse before CCH.

Interstate message switching differs from other existing and proposed national data banks because the potential for harm to individual

citizens is very large. While erroneous and incomplete information in private credit data banks may lead to credit difficulties, criminal history data of poor quality can lead to arrest and incarceration.

Even if development of an interstate message-switching capability eventually may improve data quality, there will be a transition period of several years during which the system will have to rely on data of varying quality. Consequently, the role of the CCH program in improving the quality of criminal history data should be recognized explicitly in the planning process. A plan to bring the data up to acceptable standards, to monitor the quality of data over time, and to minimize the effects of data imperfections is needed. Without such a plan, it will be reasonable for critics to question whether the system's data quality will ever come under control.

MIX OF MANUAL AND COMPUTERIZED RECORDS

The rate of records automation has varied widely among the States because of their wide differences in size, funding, and priorities. Some smaller States will probably not computerize their criminal history records for many years, if ever. A systems approach is required to deal with this difference in the speed of implementation. Allowing the computerized pointer file to contain pointers to records held by both computerized and manual states might be desirable. In any case, the CCH blueprint should deal with this aspect of the system.

SYSTEM COSTS AND FINANCING

The blueprint for the proposed system must answer a large number of cost and cost-related questions not currently addressed by the FBI. In the first instance, an estimate of costs for ***all*** system participants (or total system cost) must be included. The cost projections should distinguish between fixed costs and operational costs (entry and file maintenance costs, programing and personnel costs, and audit costs).

Second, acceptable use-cost concepts must be established. Questions of equity arise when some States who do not develop extensive CCH capability will nevertheless be able to use the files of other States who have invested heavily in a State CCH capability.

Third, the blueprint should clarify the Federal funding for the operational costs of maintaining CCH files in a manner acceptable to the existing Federal standards. Clearly, the States are resisting acceptance of Federal dedication standards, and may well resist Federal auditing requirements. Therefore, these costs may have to be assumed by the Federal Government. The current FBI plan makes only a cursory remark about auditing costs. The Department of Justice has estimated that when CCH is fully operational a permanent FBI audit staff of five people could perform the audit function, with an annual travel cost of $90,000. This estimate does not include any of the State and local auditing costs, which are likely to be much larger.

Fourth, there is an obvious relationship between distribution of costs and organizational/accountability issues which must be explored. If the States are expected to shoulder a major part of the fixed and operational costs, and if they are to bear ultimate responsibility for the adequacy of the data base with respect to a variety of criteria, then it would seem that States should have a higher level of control or authority in operation of the system than currently envisaged by the FBI. Otherwise States will be in the position of being held accountable for system shortcomings without having the authority to remedy the defects. Thus questions of cost, organization, and accountability are inextricably linked.

THE FBI IDENTIFICATION DIVISION

The FBI's Identification Division has maintained a central index of fingerprint records on criminals and manual criminal history records or "rap sheets" since 1924. These files now contain records on over 22 million people. They include not only arrestees and offenders, but military personnel, Government employees, aliens, people with security clearances, and those with voluntary personal identification cards. Until CCH, these FBI files provided the only mechanism for determining if an individual had a criminal history when an inquiring agency could find no prior record in its own State files,

The FBI will continue to respond to inquiries to the Identification Division file until "a suffi-

cient number of CCH records are amassed to satisfy operational law enforcement needs. "[23] Even if the States begin to join CCH at an accelerated rate, this period is likely to be a minimum of 5, perhaps 10, years.

Even with a decentralized CCH program, the FBI Identification Division will play a central role. While States with their own records of offender fingerprints will be able to identify offenders with prior records in the State, checks with the master fingerprint file will still be necessary if no fingerprints are on file in the State. Thus the procedure of submitting fingerprint cards to the FBI on offenders with no State record must be continued. Only in the unlikely event of extreme improvement in accuracy and cost of electronic processing of fingerprints could a centralized national file be eliminated in favor of multiple search of all State files.

The FBI is in the process of automating its identification process through a program called "AIDS" (Automated Identification Division System). AIDS will eventually provide for automatic name and fingerprint searching at the national level. While discussions with FBI representatives have clearly identified the close link between the Identification Division program and CCH, OTA is not aware of any long- term FBI plan encompassing both activities. Since it does appear that the two criminal history files will eventually become duplicative, and the fingerprint search function is so central to both, it seems necessary that long-term planning in the FBI and the Department of Justice should describe the eventual relationships. This would apply particularly to the blueprint for CCH now being prepared by the Department of Justice.

Another reason for examining both activities together is that the arguments concerning oversight and accountability for protection of individual liberties may apply with equal force to both systems. Special auditing and management procedures that may be determined to be needed for control of CCH information dissemination may therefore apply equally to dissemination of Identification Division criminal history files as well.

[23] Federal Bureau of Investigation, "National Crime Information Center—Proposed Limited Message-Switching Implementation Plan, " April 14, 1975 (Revised).

NCIC RESPONSE TIME AND DOWNTIME

There have been numerous reports of long delays, some 10 minutes or more, in response to NCIC inquiries. Furthermore, the system's downtime level is thought to be excessive. The working group received from the FBI some statistics regarding both response time and downtime." This data indicated that the NCIC central facility was unavailable to process transactions because of unscheduled downtime of an average 23.9 hours per month during the first 9 months of 1977, for an average in-service availability of 96.7 percent. There were an average of 57 outages in excess of 2 minutes in the average month. The average duration of these outages was therefore 25 minutes.

From the viewpoint of the user making inquiries to the system, this downtime results in delays at least as long as the outage. Consequently, the data suggests that over 3 percent of the NCIC transactions may have incurred delays of several minutes because of system outage. The local agency experiencing this delay receives no message explaining the nature of the problem or the delay to be expected. The user is thus left with uncertainty about the delay that is probably as operationally serious as the delay itself.

When the central processor is in service, the data provided by the FBI suggests that on the average, response time should be quite good. However, data on the peak busy period processing load would be needed to confirm this impression.

A long-term solution to NCIC'S response time and downtime problems should be addressed as part of the current FBI computer system planning and the NCIC "blueprint" exercise under way in the Department of Justice. However, it should be recognized that it is likely to be 3 to 4 years, if not longer, before these longer term plans begin to have their effect.

In the interim, the FBI has submitted a Request for Proposal (RFP) for a front-end communications controller which would be used in conjunction with the IBM 360/65 central proc-

[24] Letter from Jay Cochran, Jr., Assistant Director, FBI Technical Services Division, Nov. 10, 1977.

essor for the purpose of relieving that machine of the burden of managing the NCIC communications traffic. OTA's working group members did not conduct an investigation into the reasons for the alleged downtime and response time. However, given the data provided in the RFP and the explanation which FBI officials made of their problems, and given the technical purpose of front-end processing, and its widespread use to perform economically the general housekeeping functions associated with message control, such a procurement request would be a common technological solution toward relief of such communications problems as are described for NCIC. The procurement, however, contained a provision for message switching as a mandatory option. The FBI's stated argument for this was primarily economic: if message switching were to be authorized later, the option would have ensured minimum cost to its implementation. Inclusion of this option met strong opposition, as some saw it as a possible subterfuge to obtain message switching without authorization. The inclusion of the message-switching option ties this RFP into the CCH debate, and therefore delayed the procurement. The RFP was rewritten by the Bureau to remove all references to message switching and on April 24, 1978, was presented to the General Services Administration. As of December, procurement authority had so far been witheld pending resolution of a difference of interpretation surrounding the question of the exact nature of the procurement and procedures for obtaining it.

SOCIAL IMPACTS

Effects on the Criminal Justice System

ISSUE

In what ways, desirable or undesirable, might CCH cause, or contribute to, changes in the operation or organization of the criminal justice system?

SUMMARY

Practitioners and critics of the criminal justice system suggest that the traditional "due process" or "adversary" model of criminal justice is no longer appropriate for describing the reality of criminal justice decisionmaking. Organizational resource constraints and opportunities for discretion have increased the importance of administrative decisions in managing the workload of criminal justice agencies. CCH is an important tool supporting these mechanisms.

In the long term, CCH has the potential either to improve the quality of criminal justice decisionmaking or to introduce further inequities in the system. Careful investigation of its potential impact on administrative procedures is required.

QUESTIONS

1. Will the proposed CCH system strengthen trends towards administrative justice as opposed to traditional conceptions of legal due process, presumption of innocence, and full, fair, and open hearings?
2. What is the likely effect of the proposed CCH system on the administrative process and relationships between criminal justice agencies?
3. Will the proposed CCH system make it more difficult for former offenders to reintegrate into society and thus impede their rehabilitation?
4. What is the likely impact of use of CCH in criminal justice decisonmaking on caseloads, detention and prison populations, and requirements for judges and attorneys?

DISCUSSION

It is widely recognized by those who have examined the criminal justice system in detail that traditional, legal definitions of "due process" no longer characterize the bulk of criminal justice system activities. Such conceptions would re-

quire a presumption of innocence and truly adversary proceedings, full, fair, and open judicial hearings, free from even the taint of coercion, threats, or considerations of advantage either to the accused or the justice system. While a few accused criminals do receive such treatment, the vast bulk of the 5 million or so persons reported arrested annually do not. In most jurisdictions, from Manhattan to rural Wisconsin, over **90** percent of the convictions result from guilty pleas .25

Police officials, criminal lawyers, judges, and scholars, who have observed the reality of criminal justice decisionmaking have characterized this system, variously, as "bureaucratic due process, "[26] [27] "organizational due process, "2[8] the "crime control model, "[29] and in the popular press as "assembly line justice. "[3]o

At the heart of each of these descriptions is the notion that the criminal justice process operates under a presumption of guilt. The goals of the criminal justice agencies are rational/instrumental goals. The criminal justice process—in this view—is seen as a screening process in which each successive stage—pre-arrest investigation, arrest, post-arrest investigation, preparation for trial, trial or entry of pleas, conviction, disposition—involves a series of routinized operations whose success is gauged by their tendency to efficiently pass along cases to the next agency.

The period of the 1960's is very important for understanding current trends in criminal justice administration. It was a period of growing public awareness and fear of crime. This in turn brought crime to the foreground **as** a political issue, resulting in, among other things, a Presidential Commision on Law Enforcement and Administration of Justice. It was a period of social strife among whites and blacks, and between anti- and pro-Vietnam War proponents. The activities of the police in particular were a focus of national attention both by those who saw them as brutal defenders of the status quo, and others who wanted to solve the crime problem by removing all constraints from the police. It was also a period of increased reports of crime, increased arrest activity of police, and resultant pressures on prosecutors, courts, and prisons to administer the large caseloads. The President's Commission released a report in 1967, *The Challenge of Crime in a Free Society,* which itself became an important trend-setting document both in terms of future policies and value assumptions on the control of crime.

The report recognized that criminal justice administration in this country is highly fragmented. Each of the 60,000 agencies involved had its own recordkeeping practices and needs. This observation contributes to the pressure for computerized criminal histories as a management tool for tracking persons through the maze of the justice system.

The report also recognized the problem of recidivism. About 68 percent of persons arrested for felonies the first time will be arrested at least one more time for a subsequent felony. This has added impetus to a program of computerized criminal histories both at the State and national levels, and also has led to the development of "careers in crime" programs both at the FBI and local levels which seek to ensure that repeat offenders are dealt with severely by prosecutors and judges.

The Commission also reported a lack of information, poor management, and lack of cooperation among agencies. This encouraged the establishment of new funding mechanisms to entice local agencies into compliance with Federal and State executive branch programs.

The recommendations of the President's Commission led to the rapid development of State CCH programs; criminal histories have come to play a central role in the administrative justice process. The nature of the treatment that an individual receives from the criminal justice system has come to depend strongly on the administrative screening of his criminal history records at numerous points in the process. (See *lnforrnation Needs,* p. 17, for discussion of the

25Donald J. Newman, "Pleading Guilty for Considerations: A Study of Bargain Justice, " *)ourrza/ OJ Criminal Law, Criminology, atld Police Science* 46 (1956): 780.

ZbAb$_{ra}$h$_{am}$s. Blumberg, *Criminal)ustice,* Chicago: Quadrangle Books, 1970.

"Arthur Niederhoffer, *Behind the Shield,* Garden City, N. Y.: Anchor Books, 1969.

'"lerome Skolnick, lustice Without Trial, New York: Wiley, 1967.

"Herbert L. Packer, *The Limits of the Criminal Sanction,* Stanford: Stanford University Press, 1968.

'"Jerome Skolnick, *Justice Without Trial, New* York: Wiley, 1967.

constitutional rights and data quality issues involved here.) Thus, CCH is an important, and sucessful tool supporting the gradual shift towards bureaucratic criminal justice processes. As the use of computerized records becomes more widespread and the workload of criminal justice agencies continues to increase, further applications of CCH as a management tool can be anticipated.

The availability of criminal history records to support criminal justice decisionmaking will necessarily change the quality of those decisions. To take just one example, consider the use of CCH to aid the decision to set bail. This will operate to increase the probability that persons with criminal histories meeting certain criteria would be detained. Two alternative consequences would flow from this result. Either detention facilities would become increasingly overcrowded or incarcerating officials would adjust their decisionmaking process so that some people who would be detained under current procedures would be permitted bail.

This sort of shift in decisionmaking might be in the direction of a more rational, fair, and explicit system, allowing officials discretionary decisions to be factually based on appropriate information about the individual involved. Certainly studies show that, at present, great inequities are observable in decisions for reasons having to do with social class, ethnicity, and a host of other nonlegal social distinctions.[31] But it is also possible that one set of inequities will be replaced by another. For example, use of incomplete, inaccurate criminal histories has been attacked as systematically unfair in a current court case. [32] A future assessment could examine the effect of CCH on this trend.

The Dossier Society

ISSUE

To what extent, if any, might CCH contribute to the growth of Federal social control, or become an instrument for subversion of the democratic process?

SUMMARY

Some possible consequences of new technological systems are of such magnitude that, even though speculative and remote, they deserve serious attention, particularly if the consequences have the potential to be irreversible. Falling into this category is the possibility that CCH might become part of a drift in bureaucratic growth leading to ever larger instruments of Federal social control, or even to internal subversion of the normal democratic process.

More explicit technology contingency assesment is required to permit evaluation of this issue.

QUESTIONS

1. To what extent, if any, does the proposed CCH system in combination with other Federal systems in the Internal Revenue Service, Social Security, HEW, and other agencies expand the potential surveillance capacity of the Federal Government beyond reasonable limits?
2. To what extent, if any, will the development of a national interstate CCH capability expand criminal justice demand for and use of CCH records?
3. Given the potential for linkage between the proposed CCH system and the many other, new, massive Federal data banks, to what extent is it advisable for Congress to establish an agency specifically charged with monitoring or controlling these systems?
4. Are the available oversight and auditing mechanisms strong enough to alert society to adverse consequences in time to avoid or reverse them?

DISCUSSION

Although American society rejected the idea of a national statistical-administrative data bank, it is apparent that through incremental *decisions* in a number of areas—HEW, Internal Revenue, Social Security, Occupational Health, and so forth—the building blocks of a national data bank are, or shortly will be, in existence. It is well known that the demand for information is often encouraged by the supply of cheap, reasonable quality information. And it is con-

[31] Charles Bahn, "Sentence Disparity and Civil Rights, " U.S. Commission on Civil Rights, December 1977.
[32] Tatum, et al. vs. Rogers.

ceivable that through the pressure of day-to-day administration of large Federal programs, or through popular political pressure, certain groups of Americans will be routinely tracked through Federal data banks. Fathers who have abandoned their families provide an interesting example of a group thought particularly antisocial by Federal welfare officials, the public, and Congress. The recent program established by HEW to compare local welfare records with Federal social security files in order to track down these fathers illustrates how a combination of political and administrative forces responds to the supply of information. Such a program would be inconceivable without extensive computerization of State-1ocal welfare files. Moreover, there are no inherent limits on this process: popular passions, fed by the technical capability and supply of information, may gradually extend the dossier society to many population subgroups.

In such a context, CCH must be considered another important building block for a national data bank. The extensive use of CCH in law enforcement, criminal justice, employment, and licensing could be extended beyond present limits under pressure of new perceived needs. For example, CCH and the NCIC wanted persons and missing persons files could be used to assist in tracking and locating individuals exercising first amendment rights, and identifying members of political groups.

In exploring these possibilities, perhaps the limiting case is the possible abuse of CCH, and other systems with files on individuals, through internal subversion of the democratic process and/or cultural draft towards a bureaucratic leviathan. In the recent past, reports and hearings show that the existence of FBI criminal files, as well as some other Federal Government files on individuals, has proven a powerful temptation for some political executives to abuse the democratic process and threaten the civil liberties of Americans. In some instances, Federal administrators and other personnel with direct responsibility for the integrity of these information systems have indicated they often felt powerless or acted in concert with the abuse of these systems.

These possibilities may seem remote, but the magnitude of their consequences could be catastrophic. Furthermore, the ability of our social organization to recognize and control the incremental growth of data banks has not been firmly demonstrated to say the least.

A future assessment should examine the vulnerability of CCH to these abuses, and the prospects of strengthening safeguards against them.

Privacy and Civil Liberties Trends

ISSUE

Is there a conflict between maintaining national privacy and civil liberties trends and decentralizing responsibility for the CCH system?

SUMMARY

The national dialog on computerized criminal histories has produced some slow progress towards achieving a recognition of the need for restrictions on the dissemination of records. The effect on the health of this movement of a possible decentralization of CCH to the States is not clear. It may become more difficult to maintain a national spotlight on these sensitive questions.

QUESTIONS

1. What would be the impact of decentralization of CCH on the opportunity for oversight of constitutional rights protection throughout the country?
2. Would it be more or less possible for interested groups to focus attention on violations or patterns of governmental abuses?
3. Would a decentralized system be more or less responsive to the privacy concerns of individuals?

DISCUSSION

The creation of a computerized file with criminal histories under Federal auspices has offered a unique opportunity to make some slow national progress toward achieving social goals of fairness, privacy, and freedom of information through statutory and administrative restrictions on abuses in use of personal records and on careless or malicious or unwise dissemination of records. It allowed, indeed forced, a long-needed dialog on the need for relevancy,

accuracy, and timeliness of information on people when it was used by those agencies which most intensely exercised the force of government. Many hundreds of studies, articles, essays, and speeches have analyzed the implications of these issues which were inherent from the beginning of NCIC/CCH.

Although reflecting diversity, this dialog, and the laws, rules, and judicial decisions it generated, moved the Federal and many State governments very far along the way towards a national information policy. In itself, it has helped to weld together the diverse political arenas in our society where these issues were debated. It energized reforms in other areas of recordkeeping and many of these are documented in recent reports of the Privacy Protection Commission.

Some analysis needs to be given to the health of this movement insofar as **law** enforcement, criminal justice records and computerized systems are concerned. Returning CCH files to the States or to another entity, under different umbrellas, might reduce the opportunity for oversight of the way important constitutional rights interests are being protected throughout the country. It is not clear whether interested groups would find it easier or more difficult to turn a spotlight on a violation or pattern of governmental abuses with the intensity sufficient to effect changes. Restructuring of NCIC might result in throwing such political interest groups into an arena dominated by influential police chiefs and political executives in the law enforcement and criminal justice agencies of each State. On the other hand, such a scenario might make it easier to advocate changes and promote oversight in areas of concern to constitutional rights groups and others concerned with maintenance of effective criminal justice systems.

A future assessment of this issue should **take** notice of identifiable trends in public attitude concerning civil liberties, fear of scientific-technological development, and towards increased levels of powerlessness and alienation with regard to political institutions. Such trends are evidenced by numerous surveys, reports, and legislative activities.

Appendixes

APPENDIX A

Letters of Request

NINETY-FIFTH CONGRESS

PETER W. RODINO, JR. (N.J.), CHAIRMAN

JACK BROOKS, TEX.
ROBERT W. KASTENMEIER, WIS.
DON EDWARDS, CALIF.
JOHN CONYERS, JR., MICH.
JOSHUA EILBERG, PA.
WALTER FLOWERS, ALA.
JAMES R. MANN, S.C.
JOHN F. SEIBERLING, OHIO
GEORGE E. DANIELSON, CALIF.
ROBERT F. DRINAN, MASS.
BARBARA JORDAN, TEX.
ELIZABETH HOLTZMAN, N.Y.
ROMANO L. MAZZOLI, KY.
WILLIAM J. HUGHES, N.J.
SAM B. HALL, JR., TEX.
LAMAR GUDGER, N.C.
HAROLD L. VOLKMER, MO.
HERBERT E. HARRIS II, VA.
JIM SANTINI, NEV.
ALLEN E. ERTEL, PA.
BILLY LEE EVANS, GA.
ANTHONY C. BEILENSON, CALIF.

ROBERT MCCLORY, ILL.
TOM RAILSBACK, ILL.
CHARLES E. WIGGINS, CALIF.
HAMILTON FISH, JR., N.Y.
M. CALDWELL BUTLER, VA.
WILLIAM S. COHEN, MAINE
CARLOS J. MOORHEAD, CALIF.
JOHN M. ASHBROOK, OHIO
HENRY J. HYDE, ILL.
THOMAS N. KINDNESS, OHIO
HAROLD S. SAWYER, MICH.

Congress of the United States
Committee on the Judiciary
House of Representatives
Washington, D.C. 20515
Telephone: 202-225-3951

GENERAL COUNSEL:
ALAN A. PARKER

STAFF DIRECTOR:
GARNER J. CLINE

ASSOCIATE COUNSEL:
FRANKLIN G. POLK

September 12, 1977

Senator Edward M. Kennedy
Chairman of the Board
Office of Technology Assessment
119 D Street, N.E.
Washington, D. C. 20510

Dear Senator Kennedy:

The House Committee on the Judiciary , Sub - Committee on civil and Constitutional Rights, pursuant to its legislative and oversight responsibi1ities over the FBI , is currently undertaking a study of the FBI's criminal justice informatrion systems and related matters. The Committee has been interested in this area for some time , most recently in connection with the Bureau s request to the Department of Justice for new equipment and mess age switching capability for its National crime Information Center. The Subcommittee has focused its attention on the systems cost-effectiveness, efficiency, security and privacy protections . In addition, the larger issue of what should be the role of the federal government in this exchange of information by and for local law enforcement agencies has been raised.

In view of the technical complexity of nationwide computerized information and telecommunications systems, the Committee would like to have the assistance of the Office of Technology Assessment. In particular, we believe that OTA'S assistance would be most helpful in addressing the following issues:

1. Evaluation of the Bureau's NCIC system in terms of benefits to the users, accuracy of the data, speed, efficiency and reliability.

2. The Department of Justice is currently developing a proposal with both short and long range plans for the future of NCIC, the FBI's role in law enforcement telecommunications systems and message

switching generally. An analysis of the proposal is needed in terms of the issues raised above, i.e.:

does the proposal call for implementation of the newest and best technology available (Is that technology necessary to carry out the functions described in the proposal?);

does it provide for appropriate privacy and security measures and safeguards for constitutional rights and civil liberties; .

does it take into account the needs of its primary users, the states, on an ongoing basis;

does it or should it, provide for systematic audits of the system, both internal and external, announced and unannounced;

will it improve the speed of response and reduce the current downtime levels, both of which are cited as problems by some users and outside computer experts (Are these in fact serious problems?) ;

does it strike the appropriate balance between state and federal control of this system, keeping in mind that the Subcommittee leans toward the least intrusive federal (FBI) involvement possible, consistent with efficient operation of the system.

These questions and issues are not meant to be all-inclusive. For example, in a report prepared for the Subcommittee by the Scientists' Institute for Public Information, a copy of which is enclosed, additional problems were cited, and suggestions for change were made. Your evaluation of those problems and suggestions would also shed much light on this inquiry. Finally, your answers to all of these questions may, in turn, lead YOU to identify and assess alternatives, which would be useful to the Subcommittee's study.

Your assistance in this matter would be greatly appreciated. We look forward to hearing from you in the near future.

Sincerely,

PETER W. RODINO, JR.
CHAIRMAN

Don Edwards
Chairman
Subcommittee on Civil and Constitutional Rights

SCIENTISTS INSTITUTE FOR PUBLIC INFORMATION
355 Lexington Avenue
New York, N.Y. 10017
(212) 661-9110

TASK FORCE ON SCIENCE AND TECHNOLOGY IN THE CRIMINAL JUSTICE SYSTEM
Project on Criminal Justice Information Systems

Report on inspection and briefing at the National Crime Information Center, July 12,1977, and follow= up, August 2,1977.

Prepared by:

John J. Kennedy, Esq.
Director, Criminal Justice Task Force
August 3, 1977

On July 12, 1977, a group representing SIPI'S Task Force on Science and Technology in the Criminal Justice System performed an on-site inspection of the National Crime Information Center at Hoover FBI Headquarters in Washington, D.C. A briefing was conducted by Raymond J. Young, Assistant Section Chief, NCIC, and a lengthy question period followed. The SIPI group consisted of the following computer scientists: Daniel D. McCracken, Task Force Chairperson, and Vice-President of the Association for Computing Machinery; Joseph Weizenbaum, Professor of Computer Science, Massachusetts Institute of Technology; and Dr. Myron Uretsky, Director, Management Decision Laboratory, New York University Graduate School of Business Administration, They were accompanied by John J. Kennedy, Esq., Task Force Director, and Alan McGowan, President of SIPI. After a preliminary report of that visit was prepared, Mr. Kennedy returned on August 2, 1977 to meet with Frank B. Buell, Section Chief, NCIC, and with Mr. Young, to give the FBI an opportunity to respond to the preliminary report. As a result of that follow-up visit, some corrections were made in the preliminary report. The thirteen points discussed below represent some problem areas of the NCIC as they appeared to the SIPI group as a result of these visits.

1. There is no regular auditing of NCIC data and procedures by a relatively independent auditing authority. Department of Justice

Regulations place the responsibility for the auditing of Computerized Criminal History data on each state to perform its own audit. The NCIC Advisory Policy Board statement of October 20, 1976, also mandates systematic audits on the part of the states with respect to CCH data. There are no Regulations at all which mandate any audit of non-CCH data. Therefore, neither the FBI nor any other agency except the submitting state audits what goes into the system and how it goes in, The FBI only scrutinizes state systems when it is invited to do so by that state, or when the FBI suspects wrongdoing on the part of employees of the system. The FBI does point out errors in procedure and obvious data errors that come to its attention, However, the opinion of the Task Force was that independent auditing, both announced and unannounced, as in the case of bank audits, is crucial to maintaining the accuracy and integrity of data, and to ensure that adequate computer management practices and safeguards are being followed. For example, the rate of inaccurate records can best be determined by independent audit, but at the present time such figures for the system as a whole are unavailable. Finally, one Task Force member felt that the "friendly" relations between the local law enforcement agencies and the FBI, and the desire to keep those relations friendly, militated against a system where one part was truly looking over another part in a critical way.

2. There has been no in-depth evaluation of the actual benefits of NCIC either performed by the states or by the FBI despite 10 years of operation. Except for a number of highly dramatic incidents that are reported on occasion to indicate that NCIC works, there have been no studies, evaluations, or reports which give hard data on the benefits that have resulted to criminal justice as a result of NCIC. For example, what use does the criminal justice community make of NCIC data, and how does this improve criminal justice efforts? The actual benefits of NCIC still remain in the area of surmise, rather than demonstrated results.

3. For such a vast system, containing over $6^{1}/_{2}$ million records, with 250,000 transactions per day, the hit ratio was not demonstrated to be impressive. The system has about 1,000 hits per day, of which 50% were for stolen vehicles, 20-25 1%0 for wanted persons, and the rest scattered over the other six non-CCH files. There was no reliable data available for the CCH hit ratio. Without studies of the context of the hits, even in cases involving the "hot" files there is no proven demonstration of the significance of these hits. There is insufficient available proof of whether an extremely rapid response, which NCIC is designed to provide, is of such vital significance in a great proportion of these 1,000 daily hits. In addition, all of the information obtained through NCIC could be obtained elsewhere, admittedly, by a less rapid manner, since all the data is kept at the state level. There are other sources of criminal justice information in addition to this state maintained data. For example, there is a stolen car list maintained by a consortium of insurance companies which the FBI admits is in some respects more accurate and up-to-date than the NCIC stolen vehicle file which relies on state-supplied information. Perhaps the NLETS system, in the case of much interstate information, is an adequate, alternative communication device. The maintenance of the huge NCIC system, growing every year, may be subject to question when there is no demonstration that the 1,000 daily hits provide a significant benefit to law enforcement, and that comparable information may be available by other means, at cheaper cost, and with less significant problems involving intergovernmental relations.

4. The downtime of the system was viewed as excessive. There are about 30 hours per month of unscheduled downtime, and about 2-3 hours per month of scheduled downtime. On 7/12/77 the system had operated for eight straight days without downtime, but has had other occasions when the system was down for as long as 11 hours. It requires a minimum of 45 minutes to restart the system after downtime; it requires a cold start; and the down-

time is more due to hardware than software. Although the system has 94% uptime, the Task Force said that this would be an unacceptable record in most commercial enterprises. If such downtime existed in a bank or insurance company, it would be a situation requiring immediate corrective action. The FBI plans to request additional funds for some costly equipment upgrading, designed, in part, to solve this problem of downtime.

5. "Expungement" from the system does not mean true expungement of a record. Back-up tapes and a log are necessarily maintained by NCIC for system reliability purposes. This is a necessary precaution common in computer systems. However, since back-up tapes and a log are maintained, "expungement" ("cancellation," "clear") from NCIC really means that the expunged data is not available on-line, but does exist on tapes that are kept at FBI Headquarters. Expungement from NCIC can occur due to the fact that the initial entry was incorrect, among other reasons, but even this sort of expungement would still entail a record being maintained by the FBI, even of the erroneous data, kept on back-up tapes. The problem of expunged data does not involve insignificant numbers. For example, in a recent ten-day period, there were cancels and clears on 17,000 stolen vehicles, 2,500 CCH files, 1,000 "articles," 2,000 license plates, 6,200 wanted or missing persons, and 1,800 guns. There are a variety of reasons for these clears and cancels, but some percentage of them involve errors that put people into the files who never belonged there in the first place. Yet, these records will be maintained on NCIC back-up tapes.

6. There have been at least eight lawsuits resulting from the use of NCIC data, one of which was directed against the Section Chief of NCIC. These suits can result from false arrest, unlawful search and seizure, or other improper practices. One of the side benefits of not fully expunging data is to defend law enforcement personnel from lawsuits by pointing to data that had previously been maintained in NCIC at one time, which may have given "probable cause" for the law enforcement action that the lawsuit arose over.

7. The FBI admits that there has been poor disposition reporting by the courts. This means that arrest records remain in the system without updating of the outcome of that arrest. The arrest records do not drop out of CCH even if no disposition is ever reported. Although there are limits on the dissemination of arrest data to non-criminal justice agencies, nonetheless, data on stale arrests are not removed from the system. One Task Force member suggested that arrest data in CCH be removed unless there is prompt disposition reporting. As the system is now operated, a person will have an arrest record maintained indefinitely in CCH whether or not he is ever convicted in a court.

8. NCIC requires a cumbersome correction and updating procedure. When an entering agency corrects an error or wishes to update a record, it must transmit that data to the central state control terminal, for further transmission to NCIC central headquarters in Washington. However, in addition to the data having to pass through several different steps for correction, this procedure doesn't provide for complete correction or updating of NCIC data. For example, assume that Florida has made an input of incorrect data to NCIC, or certain data that it has input is now stale. Suppose that this is CCH data concerning John Doe. If Michigan makes an inquiry to NCIC about John Doe, Michigan will receive either incorrect or stale data. Further assume that Florida then corrects or updates John Doe's record, Nonetheless, Michigan is still in possession of the stale or incorrect data on John Doe, and unless Michigan makes another information request on John Doe, Michigan will not receive the correct and up-to-date data through NCIC. It is not possible for Florida to directly update or correct Michigan's record on John Doe through NCIC. Under current procedures, even after Florida has carried out the process of correction on-line, nevertheless, the FBI still must inform Michigan through the mails that there has been an expungement

on John Doe. There is no mail correction or updating on non-CCH files. Local law enforcement agencies are advised not to act on old NCIC hits. Only fresh hits are viewed as being adequate, and even then, the person who gets the hit must confirm this information with the entering state by another means than NCIC.

9. The procedures for the verification and certification of data by the states does not prevent at least some stale and incorrect data from being in NCIC at any given time. Every six months the FBI sends to each state either a print-out or tapes of the data that that state has submitted to NCIC that is still being maintained in the system. The state must certify that this data is correct. However, unless the state at that point takes affirmative action to correct the data sent back to it by the FBI, the data will remain in the system. That is, the state certification procedure makes the implied assumption that the data, as it is already being maintained, is correct and up-to-date. One Task Force member suggested that an alternative method would be for NCIC to periodically start with a clean slate, and have each state submit all data at that point which it could certify as correct and up-to-date. By the former method, there is an implied assumption that the data in the system is correct and up-to-date. By the latter method, no such assumption is made, and a greater burden of verification and certification is placed on each state. A second problem is that the certification procedure is carried out only every six months. This can leave a substantial time gap in the correction of records which allows a certain percentage of bad data to remain in the system during that time gap. Finally, the sanction for a state which certifies data incorrectly can include being cut-off from the system, which can also be applied in cases of improper practices of other kinds. However, because the sanction of cut-off is viewed as draconian, it is applied sparingly. No state has ever been cut off from the hot files. Only one local law enforcement agency has ever been cut off from NCIC, and that was an action taken by the State of Ohio. Three other states in the past have been temporarily cut-off from the CCH file due to reorganization of procedures in those states, but have since been restored to CCH. In a system where the only effective sanction is cut-off, the problem of enforcing procedures is a delicate one.

10. People are not informed when a CCH record is maintained on them. They do have the right to check their own file through a cumbersome process and the payment of fees in some cases, but figures were not available on the number of people who actually do check. There was some feeling expressed by Task Force members that people should be informed periodically if a record is being maintained concerning them. Address information of the people on which records are maintained appears on the fingerprint cards related to the record in CCH.

11. There are serious security and privacy considerations when between 6,6oo and 7,000 terminals can access NCIC nationwide. As the number of terminals increase, with a potential of 45,ooo local, state, and Federal criminal justice use terminals, the opportunities for abuse also increase. As long as someone can either gain unauthorized access themselves, or gain indirect access through an authorized user, a system containing sensitive data is open to abuse.

12. Despite nearly six years of operation, only 11 states are participating in the CCH portion of NCIC by providing some input, and of these, only 2 are fully participating in the sense of providing input of all arrest records. FBI Director Clarence M. Kelley, in an April 1.5, 1977 memo to Attorney General Bell, reiterated his previous request to terminate FBI participation in the CCH portion of NCIC. Director Kelley's reasons repeated his previously advanced reasons such as excessive cost of the system, lack of participation by the states, and the absence of authority for a "message-switching" capability which caused duplication of data at both the state and Federal levels. CCH records make up about 1670 of the total number of records in NCIC, yet even the head of the agency that manages the system questions the efficacy of this portion of it, and calls for the end of this portion.

13. In a May 19, 1977 memo, Peter F. Flaherty, Deputy Attorney General, wrote to Director Kelley that the Justice Department had undertaken a study to see if "interstate message switching should be authorized for the CCH program. " Message switching would entail keeping CCH data on Federal and multi-state offenders centrally maintained by the FBI, but having data on single-state offenders (about 70% of the total) maintained by the states. The FBI would keep a "pointer" file which would direct an inquiry from State X to the proper state where that CCH record was being maintained, and the capability would exist for State X to query State Y through the NCIC. The FBI would supply the facilities for a state to inquire over FBI maintained lines to each of the other states. However, this raises at least two questions. One, with direct state-to-state access, through the FBI, would there be a tremendous increase in the amount of criminal justice information that would be available on-line? For example, California's CLETS system submits only about 10% of its criminal history data to CCH, determined by the gravity of the offense, residence of the defendant, and other factors. However, with direct access, would the entire CLETS system be available to other states? The Task Force felt that as interconnection increases, problem areas multiply. Two, in this electronic context, due to the design of this central switching system, would this mean that the FBI would control the flow of ever-increasing amounts of criminal justice information throughout the country?

Appendix A

Task Force Members

Daniel D. McCracken; Ossining, New York (Chairperson)
Vice-President, Association for Computing Machinery
Consultant, and author of 14 books in computing field

Joseph Weizenbaum
Professor of Computer Science, MIT
Former member, Secretary's Advisory Committee on Automated Personal Data System, Dept. of HEW
Author, *Computer* Power *and human* Reason
(W. H. Freeman& Co., 1976)

Douglas H. Haden
Assistant Professor of Computer Science
New Mexico State University
Author, *Social Effects of Computer Use and Misuse*
(John Wiley & Sons, 1976)

Dr. Myron Uretsky
Director, Management Decision Laboratory
NYU Graduate School of Business Administration

Paul Armer; San Francisco, California
On-Line Business Systems, Inc.
Former] y at the Center for Advanced Study in the Behavioral Sciences, Stanford, California

Dr. Jerry M. Rosenberg
Professor of Management
Polytechnic Institute of New York
Author, The Dealth of Privacy
(Random House, 1969)

Dr. Robert R. J. Gallati
Northeastern University
Criminal Justice Program
Formerly, Director of the New York State Identification and Intelligence System

Jeremiah Gutman, Esq; New York, NY
Levy, Gutman, Goldberg & Kaplan
Chairman, ACLU Privacy Committee

Ronald E. Yank, Esq.; San Francisco, California
Carroll, Burdick, and McDonough
Counsel, Peace Officers Research Association of California

Anthony Ralston
Chairman, Department of Computer Science
State University of New York at Buffalo
Past-President, American Federation of Information Processing Societies (AFIPS)

Dr. Rein Turn; Redondo Beach, California
Staff Engineer, Software Analysis and Evaluation Dept.
Defense and Space Systems Group of TRW, Inc.

Professor Lance J. Hoffman
George Washington University
Department of Electrical Engineering and Computer Science

Dr. Norman H. White
Assistant Professor of Computer Applications
NYU Graduate School of Business Administration

JAMES O. EASTLAND, MI SS., CHAIRMAN

JOHN L. MC CLELLAN, ARK.
EDWARD M. KENNEDY, MASS.
BIRCH BAYH, IND.
ROBERT C. BYRD, W. VA.
JAMES ABOUREZK, S. DAK.
JAMES B. ALLEN, ALA.
JOSEPH R. BIDEN, JR., DEL.
JOHN C. CULVER, IOWA
HOWARD M. METZENBAUM, OHIO
DENNIS DE CONCINI, ARIZ.

STROM THURMOND, S.C.
CHARLES MC C. MATHIAS, JR., MD.
WILLIAM L. SCOTT, VA.
PAUL LAXALT, NEV.
ORRIN G. HATCH, UTAH
MALCOLM WALLOP, WYO.

FRANCIS C. ROSENBERGER
CHIEF COUNSEL AND STAFF DIRECTOR

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, D.C. 20510

February 15, 1978

Dr. Russe1l W. Peterson
Director
Office of Technology Assessment
Congress of the United States
Washington D. C. 20510

Dear Dr. Peterson:

It is our understanding that the Office of Technology Assessment is now engaged in a pre1iminary analysis of the National Crime Information Center in response to a request for an assessment which you received from Chairman Rodino of the House Judiciary Committee and Chairman Edwards of the Subcommittee on Civil and Constitutional Rights.

As Chairman of the Senate Judiciary Committee and as Chairmen of the Subcommittee on Administrative Practice and Procedure and the Subcommittee on the Constitution, we join in this request for a full scale assessment and evaluation of the NCIC. In view of the present and proposed role of the Federal Government in the operation and management of this exchange of information for local law enforcement agencies, we believe there is an urgent need for an evaluation of the NCIC for:(1) its benefits to the users and to taxpayers in terms of the accuracy of its data, its speed, efficiency and reliability; and (2) its consequences for effective protection of constitutional rights in the administration of justice.

The Department of Justice is currently considering various plans for updating and expanding NCIC which would include returning the computerized criminal histories (CCH) records of NCIC to the states which have already put them into the system and operating a central message switching center for local and state police agencies when they request information from other jurisdictions. This would result in a major expansion of this nation-wide system, with implications for the right of states to control local law enforcement and to develop related information systems in light of their own statutes governing privacy and freedom of information. Justice Department plans also raise major constitutional rights problems of privacy, confidentiality, security, due process and civil liberties where the technology may interact with administrative and judicial policy.

The Senate Judiciary Committee has conducted hearings and considered legislation on these issues for some several Congresses without the benefit of a thorough evaluation of exactly what information is in the system, and who needs it and why.

Especially interested in these issues is the Subcommittee on Administrative Practice and Procedure whose oversight jurisdiction encompasses both the substantive and procedural internal practices and procedures of federal agencies. The Subcommittee is strongly in favor of a comprehensive and efficient system of law enforcement, and joins with the Justice Department in seeking this goal. However, the importance of assuring a citizen's constitutional rights of due process, privacy, and civil liberties is also of prime concern.

The Subcommittee on the Constitution also has a particular interest in the NCIC. Over the past several years it has held several hearings on the issues raised by criminal information storage and retrieval systems and the various constitutional and privacy concerns presented by them. The Subcommittee has recently engaged in an, exchange of correspondence with the Attorney General on the Department's plans and intentions for NCIC.

We are, in addition, concerned with the issue of Federal control over State information, and how that issue will be dealth with in the proposed system. If the long term social consequences, beneficial as well as adverse, of this law enforcement information system are to be fully identified for Congress, we believe several areas need to be fully explored by your current working group.

First, with respect to the issue of the impact of the interrelationship of the many information policies which govern the administrative practices of Federal and State agencies which use or are affected by NCIC- -particularly by the computerized criminal history files, (CCH) ---

a. An analysis from the perspective of the right of privacy, freedom of information, due process rights and civil liberties in general should be made with respect to the above question.

b. An analysis of the Federal vs. State roles with respect to the handling of the information in the system: i.e., which person or entity will control what data in the new NCIC system, and which person or entity will be held accountable for the quality of information in the system-- and by what method this will be done.

c. An analysis should be made of the effectiveness of the policies, both for the present and future NCIC system, with respect to expungement of irrelevant, old, or inaccurate data. For instance, how would the standards for such a process be set and maintained and/or changed, if necessary? Who or what entity would be responsible for the accuracy of all records in the system? How would this be audited or reviewed in light of the right of privacy, due process and civil liberties concerns?

Second, there should be an analysis of any efforts being made to identify and address "flagging" as a potential civil liberties problem.

Thirdly, we believe that an evaluation of the efficiency of NCIC and of any proposed technological changes should encompass the effect of those changes on all other Federal users of NCIC files. This would include, for instance, the Department of Agriculture, the Veteran's Administration, Customs and the other Treasury Department Bureaus, the State Department, the Secret Service, and other interested Federal agencies. In connection with this issue, we would also like to know whether the Department of Justice plans for NCIC have considered possible alternative future relationships between those federal agencies and CCH records and NCIC data banks and computerized files.

What would be the effect on individual constitutional rights and other guarantees if the present NCIC relationships are altered? How would an enlarged system such as proposed, compare with the present system in terms of privacy, due process and civil liberties safeguards? Would certain rearrangements of NCIC tend to magnify or extend some undesirable features of the Federal use of NCIC? On the other hand, would certain rearrangements make it more difficult or costly for some agencies to use and support NCIC to the detriment of their programs and of the rights of citizens?

The fourth area which concerns us as Members of the Judiciary Committee is the relationship of NCIC programs, operations and controls to the Federal and State Judiciary. Could proposals to change NCIC tend in the long-run to fester or threaten the constitutional separation of the Judiciary from the Executive

branch and the Legislature, at all levels of government? Would pending proposals to change NCIC tend to promote or retard the ability of State judicial officials to make the most efficient use of data systems in order to protect the rights of citizens involved in the judicial process? We are not familiar with any studies that have dealt directly with this question.

Fifth, the ramifications of Federal message switching, when incorporated into such a law enforcement information system as NCIC, need to be thoroughly explored for its impact on the rights of the individual in our society, and on the powers of the States, (and on the ability of private enterprise to compete with the Federal Government) . We realize that message switching is a common technique which is useful in a great variety of government and private information programs. However, there are aspects of some of the current NCIC proposals in this area which need further study in light of civil liberties and other concerns which have been often voiced by the public and press and emphasized in Congress.

Last, but not least, we have yet to see an evaluation of the NCIC concept, that is, of whether or not an NCIC-type system is the most efficient way to accomplish the law enforcement goals desired, and whether or not we actually need a nation-wide system such as that proposed. Should private enterprise play a greater role in providing services? To what extent should the Federal government compete with private industry? An OTA assessment should, in view of your statutory mission, include an analysis of alternatives to NCIC. For instance, would an alternative arrangement be more effective in achieving our goals? How effective, for instance, would it be to develop a system iased on regional data banks? Under various alternatives, what would happen to political rights and privileges of citizens?

We believe Congress will benefit from OTA'S assessment of NCIC. This system represents the first and most important nation-wide use of computer and telecommunications technology to link federal, state and local governments, and to apply the technology to serious law enforcement and criminal justice problems of concern to our entire society. Many of the issues involved in NCIC are those common to any such Federal-State information system..

The Federal and State governments will spend millions of dollars to develop fully the NCIC and the data programs and technology which feed and support it. It is difficult, if not impossible, to reverse the effects of misjudgment or poor planning in such programs. Therefore we believe it is important to ask hard questions now and to have them resolved than to have them fester as social and legislative issues for years to come simply because governments and taxpayers have let themselves become indentured to costly and complex technology.

Sincerely,

James Abourezk
Chairman
Subcommittee on Administrative Practice and Procedure

James O. Eastland
Chairman
Senate Judiciary Committee

Birch Bayh
Chairman
Subcommittee on the Constitution

RICHARDSON PREYER, N.C., CHAIRMAN
LEO J. RYAN, CALIF.
JOHN E. MOSS, CALIF.
MICHAEL HARRINGTON, MASS.
LES ASPIN, WIS.
PETER H. KOSTMAYER, PA.
THEODORE S. WEISS, N.Y.
BARBARA JORDAN, TEX.

PAUL N. MC CLOSKEY, JR., CALIF.
J. DANFORTH QUAYLE, IND.
JOHN N. ERLENBORN, ILL.

225-3741

NINETY-FIFTH CONGRESS

CONGRESS OF THE UNITED STATES

House of Representatives

GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS
SUBCOMMITTEE
OF THE
COMMITTEE ON GOVERNMENT OPERATIONS

RAYBURN HOUSE OFFICE BUILDING, Room B-349-B-C
WASHINGTON, D.C. 20513

September 19, 1977

Mr. Daniel V. DeSimone
Acting Director
Office of Technology Assessment
Senate Annex #3
Washington, D.C. 20510

Dear Mr. DeSimone:

As Chairman of the Subcommittee on Government Information and Individual Rights of the House Government Operations Committee, I wish to confirm the previous request made by this subcommittee on September 8, 1976 for the assistance of the Office of Technology Assessment, and to seek your help in further projects of concern. The subcommittee has assignments involving the field of computer technology and other means of electronic communications which flow from our legislative jurisdiction, particularly from the mandates of the Privacy Act of 1974 and the Freedom of Information Act.

The earlier request, a copy of which is attached, was in connection with the need for technical support for the Congress in its review of Executive agency proposals to alter or establish information systems. That OTA can perform an important service in this area is clear from its assessment of the proposed Tax Administration System. OTA involvemen't on a more regular basis would, of course, be most desirable. In this regard, I and my staff would welcome the opportunity to discuss this matter with you.

Of equal, if not greater importance is the subcommittee's concern over the impact of technological advances on the development of government information programs in general. Our interests in this area would, I believe, be best served through listing the subcommittee as a sponsor for the upcoming OTA exploration of the need for a government-wide policy on computers and telecommunications. This sponsorship would afford ample opportunity for subcommittee input on those aspects of the exploration study which relate to our jurisdiction.

Thank you for your consideration and continued cooperation.

Sincerely,

Richardson Preyer
Chairman

NINETY-FIFTH CONGRESS
Congress of the United States
House of Representatives
GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS
SUBCOMMITTEE
OF THE
COMMITTEE ON GOVERNMENT OPERATIONS
RAYBURN HOUSE OFFICE BUILDING, ROOM B-349-B-C
WASHINGTON, D.C. 20515

September 8, 1976

Emilio Q. Daddario, Director
Office of Technology Assessment
119 D Street, N.E.
Washington, D.C. 20510

Dear Mr. Daddario:

The Subcommittee on Government Information and Individual Rights of the House Government Operations Committee, which I chair, has assignments involving the field of computer technology and other means of electronic communications which flow from our legislative jurisdiction, particularly from the mandates of the Privacy Act of 1974 and the Freedom of Information Act.

The Privacy Act of 1974 requires the departments and agencies to make provisions in their information systems for observing privacy, confidentiality, security of systems, and certain due process rights of the individual with respect to personal records, and for recognizing certain principles of good administration in agency record-keeping. Reports to Congress are made for each major alteration or new information system, indicating how these administrative values are incorporated in the data system and in the information practices.

Although the Act requires reports to Congress, it does not provide for the logistical scientific support needed for a qualitative review of these reports. The proposals are usually drawn by computer scientists in technological terms and frequently give only pro forma recognition to those operational areas of concern to Congress when it passed the Privacy Act. The preliminary reviews afforded them within the agencies and the Office of Management and Budget, as well as the review afforded in the appropriations process in Congress address economic and technical feasibility problems, unless the proposed data system would result in a glaring violation of individual privacy. However, the very complexities of these systems may disguise significant changes. Important administrative and constitutional values of privacy and due process may be affected by the technology as it is applied to various programs unless certain technical and administrative guarantees are established in advance.

As new technology becomes available and existing systems are strained, billions of dollars will continue to be spent on these new or expanded data systems. Due to their size and complexity, any errors or negative impacts on individual rights in the operations of federal programs will be expensive and difficult to correct. It is important therefore that on certain vital issues the union of the technological and policy dimensions be established from the beginning, and it is not at all clear that this is currently being done or will be done in the future. I believe that effective oversight by Congress must incorporate these two elements and must result in institutionalizing it at some point in the process.

This search for the union of policy and technology seems to me to be a particularly appropriate area in which the Subcommittee might benefit from the advice and assistance of the Office of Technology Assessment. Congress sorely needs education and help in its evaluation of these scientifically-oriented systems reports, and it appears to be precisely the type of project for which the OTA is uniquely suited.

For example, the proposal for a new Tax Administration System is one such report on which the Subcommittee would welcome the advice or recommendation of the Office of Technology Assessment with respect to the adequacy of the Internal Revenue Service's stated guarantees concerning privacy and other individual rights.

I and my staff would welcome the opportunity to discuss with you the possibility of receiving OTA's technical assistance on a regular basis, or its advice in developing a format for the Subcommittee's routine consideration of those aspects of the agency systems reports filed with the Government Operations Committee which relate to our jurisdiction.

Your cooperation is deeply appreciated.

Sincerely,

Bella Abzug

BELLA S. ABZUG
Chairwoman

APPENDIX B

Pertinent excerpts from the Department of Justice Report: *Representative Viewpoints of State Criminal Justice Officials Regarding the Need for a Nationwide Interchange Facility.* March 6,1978

QUESTIONS PRESENTED AND SOURCES OF INFORMATION

In order to ascertain the needs of the criminal justice community, the Department of Justice and subcommittee staff officials visited 10 States during the period November 1977 through February 1978. The States visited were California, Florida, Georgia, Illinois, Massachusetts, Minnesota, New York, North Carolina, Texas, and Wisconsin. Department of Justice and subcommittee staff officials believed these States to have both representative qualities and relevant experiences in terms of the issues to be considered.

Specifically, while all of the States routinely used National Crime Information Center (NCIC) facilities in acquiring information for wanted persons, wanted properties, etc., all of the States also had fully developed State capabilities for the intrastate exchange of this type of information. All of the States had regular access to the NCIC-Computerized Criminal History (CCH) file, but only five States were "full" NCIC-CCH participants in that they were NCIC-CCH record contributors. Conversely, and for various reasons, five of the States were not contributing records to the NCIC-CCH file.

Indeed, these 10 States offered particularly valuable insights with respect to the NCIC-CCH issues because of the variety of experiences they had acquired in dealing with the CCH program at the State level; e.g., some States had a high degree of success in implementing the present CCH concept while other States had less success; some States were eager to participate in the NCIC-CCH program, while other States conditioned future participation on the need for a clear position being taken by the Federal Government, i.e., an unqualified commitment to the CCH concept.

Further, these States possessed representative qualities in terms of requisite criminal identification capabilities. Specifically, several States had already adopted and implemented progressive measures and capabilities, such as the: *single source* submission of fingerprint cards to the Federal Bureau of Investigation (FBI) Identification Division; the *single card* submission (i.e., the submission of a card only when the identity of the subject was questionable, etc.); while other States were only beginning to recently address the need for a modern State-level identification facility as a corollary to the effective statewide management of criminal records.

In the course of these visits, the Department of Justice and subcommittee staff officials asked State criminal justice officials a series of questions dealing with the needs of the specific State which the officials represented, and how such needs might best be satisfied. The principal questions were:

1. In discharging intrastate criminal justice responsibilities, is it necessary to acquire out-of-State criminal justice **data for (a) wanted persons, (b) wanted properties, and (c) prior criminal offenses?**

2. If it is necessary to obtain out-of-State information for (a) wanted persons, (b) wanted properties, or (c) prior criminal offenses, which data could be obtained satisfactorily by means of bilateral agreement between States? Which of this data could be obtained reasonably by means of regional arrangements? Must any of this data be the subject of a routine nationwide inquiry?

3. If a nationwide information interchange facility is required to exchange criminal justice information for (a) wanted persons, (b) wanted properties, or (c) prior criminal offenses, what is the proper and preferred role of any participating Federal agency? That is, should the role and responsibility of a participating Federal agency be similar to that of a participating State, or should the participating Federal agency have responsibility for the administration of the nationwide criminal justice information interchange facility?

4. If a Federal agency is to be responsible for the administration of a nationwide criminal justice information interchange facility, should that agency be one which does not have operational law enforcement responsibilities? More specifically, if a Federal agency is a proper and preferred agency to administer such a facility, should that responsibility be vested in the FBI?

5. What changes, improvements, etc., are needed in terms of the existing capabilities, procedures, etc., which govern the inter jurisdictional exchange of criminal justice information? What problems, if any, are associated with the present criminal identification process in which local criminal justice agencies submit identification requests directly to the FBI? Are the present methods of processing such requests adequate and responsive to the needs of the State criminal justice community? What alternative methods would be preferable?

6. Do the present methods associated with the collection, storage, and exchange of criminal records afford State officials adequate control over access to, and dissemination of criminal records? What, if anything, must be done to remedy any existing shortcomings?

RESPONSES OF STATE CRIMINAL JUSTICE OFFICIALS

Without exception, all of the State officials agreed that the convenient and rapid acquisition of out-of-State data pertaining to wanted persons, wanted properties, and prior criminal offenses was essential to the proper discharge of their statewide responsibilities. State officials emphasized the increasing level of contact between criminal justice authorities in their States with nonresidents, and offered convincing arguments that the equal treatment of offenders is in part dependent upon the equal availability of appropriate and relevant information at all stages of the criminal justice process,

With respect to the acquisition of criminal justice information, State officials emphatically rejected bilateral or regional arrangements for a variety of reasons. Frequently, the State officials cited shifting priorities within many States as a result of changes in administration, the tensions which occasionally arise between neighboring States, the fact that offenders with whom State criminal justice officials come in contact are not exclusively from any particular grouping of States, the constraining experiences and limited success associated with previous localized or regional undertakings, etc.

In strongly endorsing the need for a nationwide reference (index) capability for wanted persons, wanted properties, and prior criminal offenses, State officials repeatedly and without exception expressed a preference for a federally administered facility. The State officials frequently pointed out that a federally administered facility is “neutral” in terms of its dealings

with State agencies and tends to be uniformly responsive to all States. Further, recognizing the sensitivity of the subject matter which would be processed by such a facility, many State officials expressed the view that a federally administered facility would be subject to greater scrutiny and hence, would more likely be in compliance with existing laws, regulations, and policies than a facility administered by a non-Federal entity, such as a consortium of States, etc., (In responding to this particular question, State officials were asked to assume that Federal funds would be available to any nationwide servicing facility, whether administered by a Federal agency, or otherwise.)

While many State officials expressly or implicitly recognized that in the longer term a Federal **agency** other than the FBI could provide the services expected of a nationwide criminal justice information interchange facility, there was a clear consensus that the FBI should continue to provide such services in the foreseeable future. The State officials repeatedly stated that notwithstanding creditability problems which the FBI might have with some public or private organizations, officials, etc., it enjoys substantial creditability within the criminal justice community in terms of professional qualifications and capabilities. Some State officials appeared to be of the opinion that the question of the FBI's lack of creditability within the community at large is exaggerated, and insofar as they were concerned or insofar as the citizens of their State might be concerned, it was not a significant public issue. Nevertheless, virtually all of the State officials recognized the problems confronting the FBI, but believed that the establishment of proper oversight measures would be an appropriate response to most criticism of present or future servicing arrangements.

However, State officials were outspokenly critical of the Federal Government generally, and specifically of the Department of Justice, the FBI, and to a lessor extent, LEAA. Each of the following criticisms was frequently expressed by officials in many of the 10 States which were visited, and in some instances, the criticism was encountered in every State. The most important criticisms addressed:

1. The indecisiveness of the Federal Government in terms of its support for both NCIC generally, and the CCH program specifically. State officials frequently spoke of the degradation of NCIC services in recent years, and the apparent inability of the Department of Justice to establish a clear direction for the CCH program, In this regard it was learned that a number of States which are not presently contributing CCH records to the national system have already established operational CCH capabilities at the State level and are ready to participate in a decentralized CCH program. However, they will not do so until a clear policy decision is reached by the Federal Government.
2. State officials were critical of fragmented responsibility within the FBI with respect to criminal history records. Some were particularly critical of the fact that the Identification Division "rap sheet" operations was organizationally separated from CCH program operations; that neither the Identification Division, the CCH program, nor the NCIC Section of the FBI had authority to establish effective and binding priorities for system services; that the automatic data processing services, telecommunications services, etc., which support the activities of the States were subject to a decision process in which internal FBI needs were addressed *vis-a-vis* the needs of the States, etc.
3. The need to remedy a long-standing source of difficulty associated with the direct, routine, and frequently unnecessary submission of fingerprint cards from the arresting agency to the FBI Identification Division. Specifically, officials in every State endorsed an improved procedure by which arresting agencies within their State would submit fingerprint cards to the *State Identification Bureau,* and the State Identification Bureau would only forward to the FBI Identification Division fingerprint cards pertaining to persons whom the State Identification Bureau could not definitively identify (first-time offenders within that State, persons using an alias, etc). State officials strongly supported the proposal that where the identity of the arrestee was not at issue because of a prior contact with State

criminal justice authorities, etc., the practice of routinely submitting fingerprint cards to the FBI should be discontinued. (State officials did recognize that this would, in many instances, require States to accept increased responsibility for managing the criminal identification process as well as increased responsibilities in terms of criminal records operations. State officials also pointed out that this would require the cooperation of the FBI Identification Division. Various State officials acknowledged that the FBI had been generally supportive of such efforts, but several officials indicated that occasionally the FBI Identification Division has been less than fully supportive of innovations of this kind.)

4. The present methods governing the interjurisdictional exchange of criminal records, stressing that it is not meeting the needs of State and local criminal justice agencies. That is, when an arresting agency forwards a fingerprint card to the FBI, the typical elapsed time before the arresting agency receives any response is in excess of 2 weeks. State officials time and time again stressed the growing needs of criminal justice officials such as prosecutors, magistrates, judges, etc., for more timely responses. The officials emphasized that such responses were no longer expected in timeframes such as weeks, days, or even hours; rather, some officials expressed the view that data pertaining to prior out-of-State criminal offenses must be immediately available. While not all State officials set so formidable a requirement, all State officials did express the view that such data must be available within hours if they are to comply with the emerging expectations of the States which they serve. (It should be noted that this level of system response was discussed in terms of prior *criminal offense data only.)* All State officials believed that virtually instantaneous access/response was absolutely essential in terms of wanted persons, wanted properties, etc. And, in this regard, all of the officials believed that the Federal Government generally, and specifically the Department of Justice, the FBI, NCIC, etc., were failing to support properly the various State criminal justice communities which NCIC was established to serve.

5. The lack of State control over State criminal records presently held in the central repository maintained by the FBI Identification Division. In this regard, it is necessary to recognize that the manually maintained criminal record, or "rap sheet, " now held in the central repository, is a composite chronological listing of offenses/dispositions associated with a particular individual. Offenses/disposition from multiple jurisdictions may be included in any particular record, and this criminal record is updated and released by the FBI whenever an authorized agency makes a request for the records. This practice has become particularly objectionable to officials in States which have enacted legislation mandating strict State control over access and dissemination of criminal records.

6. Many, although not all State officials, were critical of the composition of the NCIC Advisory Policy Board. It was frequently pointed out that while the various NCIC "want" files are of principal interest to the law enforcement community, the CCH program is of interest to the entire criminal justice community and that the NCIC Advisory Policy Board is not properly constituted for addressing CCH program requirements. (Indeed, some State law enforcement officials acknowledged that CCH was of primary interest to prosecutors, judges, court personnel associated with pretrial diversion programs, correction officials, etc., and was of only limited interest to law enforcement agencies, *per se*.)

7. Dissatisfaction with LEAA funding concepts, particularly with the "bundling" of numerous functions within the LEAA Comprehensive Data Systems (CDS) program. This program required States which wished to undertake a CCH implementation plan with LEAA funds to agree to engage in other program activities which, at least in some instances, were of interest to LEAA rather than to the State which LEAA was purporting to assist. Further in

the course of the visits to the various States, it became quite clear that LEAA never adequately comprehended or addressed programmatically the critical relationship between the criminal identification process and the interjurisdictional exchange of criminal records.

A CONSENSUS CONCEPT

Possibly because of the lingering impasse, and the spreading and intensifying dissatisfaction among officials in all of the States, officials in the 10 States eagerly analyzed and commented on alternative concepts for a nationwide criminal justice information interchange facility. There was marked agreement as to what conceptual arrangement would best satisfy the needs of the States. The concept which enjoyed the unanimous support of State officials is most easily described by a discussion of the process and procedures associated with the concept. Specifically:

Identification Procedures

1. Following an arrest the arresting agency would send/transmit the subject's fingerprint card to the State Identification Bureau. If this arrest was the first contact between the subject and the criminal justice authorities of that State, a definitive identification could not be made as the subject might have engaged in criminal activities in either the same jurisdiction under a different name or in another jurisdiction under either the same or a different name. (Note: If the State had a fully developed "technical" fingerprint search capability it would be able to make a definitive identification of all subjects who had previous contact with the criminal justice authorities of that State.) Accordingly, the State Identification Bureau would forward/retransmit the fingerprint card for each first offender (within the jurisdiction) to the FBI Identification Division in order to establish the definitive identification of the subject. In all such instances, the response from the FBI would consist of the FBI identification number assigned to the subject, and any other identities which the subject is known to have previously used.
2. The FBI identification number and such identification information as is necessary to establish the identity of the subject would be transmitted by the most rapid means to the State Identification Bureau. At that point, the State identification record could be completed, and thereafter would contain both the State identification number and the FBI identification number. State officials would then determine whether the offense was of such a nature that the existence of the criminal record should be reflected in a nationwide index. If the offense met both State and national criteria for entry in a nationwide index of decentralized criminal history records, then the State authorities would transmit, for index entry purposes only, the identification segment of the record established at the State level.
3. On all subsequent and appropriate contacts between the criminal justice authorities of that State and a person for whom the State Identification Bureau has previously created a record, the arresting agency would continue to send/transmit the subject's fingerprint card to the State Identification Bureau. However, since the State would ordinarily be able to make a definitive identification based upon prior contact, it would not be necessary to forward/retransmit the subject's fingerprint card to the FBI, nor ordinarily would the State have to take any action with respect to the nationwide index (unless there was a significant change in the identification data contained in the index, e.g., amputations, etc.)

Record-Accessing Procedures

4. In contrast to present procedures whereby each arresting agency, or authorized crim-

inal justice agency now routinely obtains "rap sheet" or CCH record data from the one or both of the centralized FBI repositories (Identification Division or NCIC-CCH files), under the revised procedures access to the criminal records of all States would be subject to multiple, albeit increasingly automated review processes. Specifically, any time an arresting agency—or a criminal justice agency making an inquiry under nonarrest procedures—wished to access a criminal record it would transmit the inquiry to its State crime information center. Each such inquiry would contain a "purpose" code as well as a "scope of search" code—indicating whether a statewide or a nationwide search was desired.

5. If a statewide search was requested or otherwise indicated, the State crime information center would process the request in accordance with State law, regulation, and policy and respond directly to the inquiring agency. No search of the nationwide index would be necessary and there would be no interjurisdictional (interstate) exchange of data.

6. If a nationwide search was requested, the State crime information center would determine whether a nationwide search for the purposes specified was consistent with State law, regulation, and policy. If so, it would log the request and retransmit it to the nationwide criminal justice information interchange facility (nationwide servicing facility). Upon receipt, message-control data associated with the inquiry would be logged at the nationwide servicing facility and a search would be executed against the nationwide index data—providing that the purpose of the search conformed to Federal law, regulation, and policy, If the nationwide index search revealed no prior entry, the inquiring State crime information center would be notified promptly, and they in turn would furnish the inquiring agency of the results of the search of State records, as well as the "no record" result of the nationwide index search.

7. If the search of the nationwide index revealed a prior entry, the nationwide criminal justice information interchange facility would further retransmit the request for the subject's criminal record (along with the identity of the requesting agency and the purpose for which the record is being requested) to each of the States to which the index "points" as being in possession of relevant criminal record information. No response would be made by the nationwide servicing facility at this stage of the process to the inquiring State crime information center, nor by it to the agency which initiated the inquiry.

8. Upon receipt of a record request from the nationwide criminal justice information interchange facility, each State crime information center which had been "pointed" to as holding relevant criminal record data on the subject would log the request and determine whether the release of the data to the inquiring State crime information center (and the inquiring agency) for the indicated purpose was consistent with its State laws, regulations, and policies. If the request met the release criteria of the State(s) holding the record, and if the data met the standards (which must be established or validated in each State) of accuracy, completeness, and currency, then the State crime information center(s) would transmit back to the nationwide servicing facility the requested information in a standardized format. Conversely, if for any reason any State holding a record declined to release a record upon which an inquiry was made, an appropriate response would be transmitted to the nationwide servicing facility. In either event each State crime information center would log its reply transmission.

9. Upon receipt of responses from the State(s) to which the nationwide index had pointed, the nationwide criminal justice information interchange facility would log message-control data associated with all replies, modify the index pointers (as necessary to conform to certain negative responses), and assemble the replies into a single integrated response to be transmitted back to the inquiring State crime information center. Message-control data associated with the integrated

response from the nationwide servicing facility, and the receipt of the message by the inquiring State crime information center would be logged.

10. Upon receipt, the inquiring State information center would further assemble the integrated response from the nationwide servicing center with any relevant data held in the subject's State record, and forward the final response to the inquiring agency.

This conceptual design of a decentralized nationwide system of criminal history records provides State officials with maximum control over State records while permitting the reasonable exchange of these records between identifiable agencies for known purposes. If implemented, State officials would be in a position to ensure compliance with State law, regulations, and policies. Most importantly, however, it pinpoints responsibility, and affords maximum auditability of either the entire system or any component part of the system.

CONCLUDING OBSERVATIONS

The brief description of a consensus concept and the accompanying procedural changes are not intended to be a definitive systems design. Rather, they are indicative of the principal features of a system which would restore a balance of responsibility among the States and the Federal Government. This balance has been absent for the past half-century in the areas of criminal identification and criminal records.

But the purpose of restoring a balance long lost is not the principal reason why corrective action should be taken immediately. Rather, the more compelling reasons arise from the indefensible situation which presently exists; that is, a situation in which State criminal records are maintained in a fashion which does not put State and local criminal justice agencies in the best position to ensure the accuracy, completeness, and currency of State criminal records; a situation in which the response to a record request is so lengthy in term of elapsed time that it works to the advantage of the career criminal and to the disadvantage of the first offender; and a situation which affords State officials virtually no effective control over dissemination of State criminal justice data.

If this situation existed under circumstances where it was the best that our society could do, it would be unfortunate; for it to exist in a society such as ours, where we know we can do much better, there is no reason for further delaying the necessary corrective efforts.

In terms of corrective measures, the next logical step would be for the Department of Justice to acquire validating endorsements of the conceptual and procedural features indicated in this report. This might best be done by the broad circulation of this report to all relevant Federal and State agencies, appropriate public and private organizations, etc. Thereafter, the next logical step would be for the Department of Justice to obtain Program and System Design Proposals. In this respect, the Department, in concert with the cognizant congressional authorities, could select a distinguished panel of State officials to develop and present for appropriate consideration the required Program and System Design Proposals. Alternately, the Department, in similar concert with the cognizant congressional authorities, could commission several qualified private organizations to develop and submit the required Program and System Design Proposals.

In either event, an unrelated panel of Department officials, congressional authorities, State officials, and other public representatives should be constituted to review and recommend implementation of the most suitable approach.

SEVERAL FOOTNOTES

This report, apart from its conclusions nd recommendations, attempts to set forth faithfully the views of many State officials on a highly controversial and important criminal justice matter. It obviously will not be pleasing to all, nor is it so intended. Nevertheless, to the degree that it reflects accurately the prevailing situation and the views of the officials in the 10 States which were visited, the public is well served.

In the interest of furthering the readability of a report dealing with a highly complex situation, detailed distinctions, amplifying commentaries, etc., have been avoided throughout the body of this report. However, several important footnotes are appropriate at this point; specifically :

1. Not mentioned elsewhere in this report is the fact that these issues were discussed with a number of general government State officials, as well as municipal and county officials, including Mr. Doug Cunningham and his associates in the California Governor's Office, Assistant Sheriffs Tom Anthony and Robert Edmonds of Los Angeles County, and Messrs. Frederick Gustin, Victor Riesau, and Richard Humphries of the Los Angeles County Sheriff's Office Technical and Detective Divisions, respectively. Further, the findings contained in this report were reported to the Board of Directors of the National Law Enforcement Telecommunications System (NLETS), Inc., and an *ad hoc* meeting of SEARCH Group, Inc., representatives. While it would be presumptuous to attribute a position on this matter to either organization, it appeared that there was a considerable level of support for the same concept and procedures which appears preferable to State officials.

2. All State officials were asked to comment on the possibility of using NLETS services in lieu of NCIC generally, or in lieu of NCIC-CCH services specifically. All officials considered such a proposal totally unacceptable and endorsed the June 12, 1975 agreement between the NCIC Advisory Policy Board and the NLETS Board of Directors. This agreement dealt with the proposed distribution of service responsibilities between the two systems. One State (Illinois) suggested, however, a minor modification to the agreement in one area, that associated with NCIC "hit" confirmation messages.

3. Most, if not all State officials believed that LEAA must address more directly the needs of the State identification functions, and the relationship between the identification process and criminal record operations. Notwithstanding the fact that LEAA has funded several attempts at innovation in this area, its contribution to the improvement of State identification capabilities is generally regarded as modest, if not meager in nature.

4. One prominent State official astutely pointed out that the NCIC Advisory Policy Board may serve a valid purpose as an advisory instrument for the Director of the FBI and might be left undisturbed so that it can provide continuing operational insights. However, this official stressed that it lacks the broad public and criminal justice community representation which is appropriate for the formulation of national policy in this sensitive area. This official recommended consideration be given to the establishment of a truly independent regulatory commission.

5. Although the description of the consensus concept in this report does not address the readiness of the various States to participate in the improved conceptual arrangement, attention has been given to this in the meetings which were held with State officials. There is no prohibitive or even formidable reason that would prevent the consensus concept from being implemented promptly by all States.

6. The representatives of the Federal Government who participated in this fact-finding effort included Messrs. T. Breen and R. Starek of the staff of the House Judiciary Subcommittee on Civil and Constitutional Rights; E. DoIan of the Department of

Justice; J. Daunt in the capacity of special consultant to the Department of Justice; J. Cochran, F. Still, F. Buell, and R. Young of the FBI; H. Bratt, and S. Ashton of LEAA; L. Bastian of the Department of Justice, and M. Lane of the Department of Treasury. Both Mr. Bastian and Mr. Lane are presently serving with the President's Reorganization Project for Law Enforcement.

7. Since footnotes have not been employed in the preparation of this report each of the participating officials indicated in footnote 6, above, have reviewed this report and have been invited to provide individual concurring, dissenting, or amplifying comments. By and large, the comments which have been received were orally communicated, and have resulted in modifications to the language employed in earlier drafts of this report. Written comments received by March 3, 1978, are attached.

APPENDIX C

Chronology of CCH

(This chronology describes some NCIC/CCH events brought to public attention by the press and Congress. It is by no means complete. A more definitive list would form part of the formal OTA assessment.)

February 1967
The President's Commission on Law Enforcement and the Administration of Criminal Justice recommends use of computer technology by criminal justice information systems on a decentralized basis.

July 1969
Project SEARCH, a consortium of 10 States receiving LEAA funds, is created to develop a prototype computerized network to exchange criminal history information on a decentralized basis.

July 1970
Project SEARCH privacy report is issued, calling for adoption of restrictions on criminal history data collection to safeguard privacy.

October 1970
Mathias Amendment to Omnibus Crime Control and Safe Streets Act of 1968 requires LEAA to submit legislative recommendations to regulate the exchange of criminal justice data.

December 1970
Attorney General Mitchell authorizes FBI to take control of the Project SEARCH criminal history index.

June 1971
Menard *vs.* Mitchell decision limits dissemination of FBI arrest records outside the Federal Government.

September 1971
S. 2546, LEAA's recommendation pursuant to the Mathias Amendment, is introduced. It gives the Attorney General broad power to determine access to criminal justice data banks. No action is taken on the bill.

November 1971
FBI announces that it has added the nationwide criminal history data bank to NCIC.

November 1971
Bible Rider to the Supplemental Appropriations Act of 1972 gives FBI authority to continue dissemination of arrest records negating the effect of the *Menard* decision.

January 1973
GAO report says Department of Justice has not determined costs of developing a fully operational CCH system, thus preventing States from determining whether they can afford to participate. Also, users have no assurance that data entered into CCH is complete/accurate because not all arrests/dispositions are being reported by participating States. Report adds that LEAA/FBI agree with above critique but aren't doing enough to correct problems. Specifically, LEAA is collecting cost information as part of its Comprehensive Data Systems program (CDS), but not all States exchanging CCH records are required to participate in CDS, and State submissions to CDS will not show separately the costs of developing CCH exchange capability. Regarding the arrest/disposition reporting problem, GAO says NCIC'S plan to inform participating States, periodically, of the specific CCH records for which no dispositions are available, will fail to remedy "a serious system deficiency" because simply informing the States that certain records are incomplete will not prevent users from acquiring the information and acting on it despite this shortcoming.

Spring 1973
Alaska and Iowa enact statutes governing use of criminal history records.

June 1973
Massachusetts refuses to participate in the CCH program until safeguards are adopted at the Federal level. Justice Department sues to

gain access to data in the Massachusetts State files by the Small Business Administration.

July 1973

Kennedy Amendment to the Crime Control Act of 1973 requires LEAA to issue regulations controlling LEAA-funded State criminal justice data systems.

July 1973

HEW Report, *Records, Computers, and the Rights of Citizens,* is published. It proposed limitations on automated personal data systems on the Federal Government.

August 1973

Massachusetts Governor Francis W. Sargent and others petition Justice Department to develop standards governing criminal history records.

February 1974

LEAA proposes regulations to control criminal justice information systems which receive Federal funds.

February 1974

S. 2963, drafted by Senator Ervin, together with S. 2964, drafted by the Justice Department, and introduced by Senator Hruska, are referred to Senate Constitutional Rights Subcommittee. (Neither bill was enacted.)

October 1, 1974

Deputy Attorney General Silberman authorizes FBI to engage in "limited" switching of NCIC-related messages, provided the Bureau prepares an implementation plan that is approved beforehand by the Attorney General.

April 14, 1975

FBI releases a "National Crime Information Center Limited Message-Switching Implementation Plan. "

May 20, 1975

Justice Department, after redrafting regulations proposed in February 1974 on the basis of subsequent comments, publishes the new Rules in Federal Register "governing dissemination of criminal records and criminal history information. " These regulations provide privacy safeguards of individual records in files maintained and administered by the FBI, criminal justice exchange of records. Also, the regulations require State criminal history record information to be stored and processed in dedicated computer system.

June 19, 1975

LEAA regulations become effective.

July 1,1975

Senator Tunney, Congressman Edwards introduce S. 2008/H.R. 8227 to control dissemination of information from criminal justice information systems. The bills, identical to each other, include a Federal regulatory commission similar to one proposed the previous year, by Senator Ervin in S. 2963. (The Tunney/Edwards legislation was not enacted.)

October 24, 1975

Justice Department modifies regulations to let States use shared computer facilities, if proper precautions are taken. Justice also announces it will hold hearings to consider changes in provisions covering dissemination of criminal history record information.

November 1975

Attorney General Levi defers decision granting FBI permission to implement NCIC message-switching capability, after congressional critics and others express fears that agency will gain too much power,

March 19, 1976

Following December Justice Department hearings to assess balance between public's right to know such information and right to privacy, LEAA adopts amended regulations covering records dissemination and sharing of related computer systems. In effect, rules leave the dissemination up to the individual States. Each State must submit a plan describing its dissemination and security procedures. After review and approval by LEAA, these procedures must be implemented in each State by December 31, 1977. States must devise plans that comply with requirements specified in amended regulations and are allowed to use shared computers to store and process criminal history record information, provided systems satisfy criteria specified in regulations.

April 16, 1976

FBI Director Kelly requests permission from Attorney General Levi to terminate FBI participation in CCH program because the cost and effort of maintaining the centralized CCH system was "grossly underestimated, " the intergovernmental relations problems are "legion, " and the Bureau "cannot move ahead with its plans to decentralize CCH because it

does not have message-switching authority or capability. ”

April 5, 1977

FBI Director Kelley requests authority from Deputy Attorney General Flaherty to implement a new NCIC message-switching plan, unrelated to CCH. The proposed switch would provide Federal agencies “and localities such as Puerto Rico” with access to NLETS through NCIC communication circuits. It would also enable the Royal Canadian Mounted Police information center in Ottawa, Canada to access non-CCH NCIC files.

April 15, 1977

FBI Director Kelley reiterates his request to terminate FBI participation in CCH.

May 10, 1977

Congressman Edwards, in a letter to Deputy Attorney General Flaherty, suggests that the ultimate decision by the Justice Department regarding CCH and message switching should be preceded by testimony before the House Subcommittee on Civil and Constitutional Rights.

May 19, 1977

Deputy Attorney General Flaherty approves FBI April 5th proposal but cautions that “this approval should not be construed to authorize the switching of CCH messages. ”

May 19, 1977

Deputy Attorney General Flaherty advises FBI Director Kelley not to terminate FBI participation in CCH pending review of the matter by Flaherty’s staff.

June 7, 1977

Congressman Edwards asks Deputy Attorney General Flaherty to defer approval of FBI’s April 5th request for limited messsage-switching capability “until we have testimony” from the Department of Justice and other interested parties.

July 11, 1977

Deputy Attorney General Flaherty revokes his May 19th memo authorizing FBI to proceed with limited message-switching plan. Flaherty says “we are thoroughly reviewing the subject of message-switching. . . in cooperation with Members of Congress. ”

August 3, 1977

Scientists Institute for Public Information (SIPI), after evaluating NCIC at request of Edwards subcommittee, issues critical report. It alleges, among other shortcomings, that NCIC data and procedures are not audited regularly, and that the system’s actual benefits “remain in the area of surmise. ”

September 12, 1977

Congressmen Edwards, Rodino ask OTA to conduct study of NCIC for House Subcommittee on Civil and Constitutional Rights.

September 28, 1977

FBI responds to SIPI report, disagreeing with most of its findings. For example: NCIC is audited, although not by an independent agency, and it is “incorrect to say that the actual benefits of NCIC ‘remain in the area of surmise. “

September 29, 1977

Deputy Attorney General Flaherty, in letter to Congressman Edwards, proposes “interim measures” to improve NCIC operation. They include:

a) Continuing FBI participation in CCH while taking steps to decentralize the files. The first step would be adoption of **a** CCH decentralization blueprint, developed “in concert with Congress” and other interested parties.

b) Adding message-switching capability to NCIC’S computer system but not employing it until the blueprint is approved.

c) Negotiating with GAO to provide an independent NCIC system audit capability.

d) Reviewing NCIC Advisory Policy Board reporting procedures to ensure their “maximum effectiveness. ” Deputy Attorney General says he favors having Board report directly to the Attorney General or Deputy Attorney General through the FBI Director.

October 20, 1977

Congressman Edwards, answering Deputy Attorney General Flaherty’s September 29th proposal, emphasizes need to develop standards assuring that CCH records, when distributed to the States, will be protected against misuse. Congressman Edwards also says the Justice Department blueprint should consider seriously whether another agency—NLETS or some similar one—should perform message switching. He recommends that Justice consider adding “persons not directly involved in the NCIC System” to the NCIC Policy Advisory Board.

December 6, 1977

Justice Department gives States until March

1, 1978, to implement dissemination/security regulations issued in March 1976. The original deadline was December 31, 1977.

December 13, 1977

Attorney General Bell proposes abolishing LEAA and replacing it with a National Institute of Justice. The official reorganization proposal is to be submitted to Congress in the spring of 1978. Major provisions: State criminal justice plans and projects would no longer require prior Federal approval; regional criminal justice planning boards would no longer be subsidized by the Federal Government; administrative costs would be funded by the Federal Government on a more limited basis, requiring dollar-for-dollar matching by State/local recipients.

January 6,1978

SIPI responds to FBI comment on 1977 SIPI study of NCIC. "It is our considered opinion that an indepth study of NCIC, performed by the Office of Technology Assessment, the General Accounting Office, a qualified independent organization, or all three is called for."

95th Cong., 2d Session: No legislation was enacted. Hearings and studies continued on LEAA restructuring and guidelines before the House Judiciary Subcommittee on Crime and the Senate Judiciary Subcommittee on Criminal Laws and Procedure. The full Senate Judiciary Committee also conducted hearings and studies related to the FBI statutory charter. This subject is also of concern to the House Judiciary Committee.

APPENDIX D

Glossary

AIDS—''Automated Identification Division System," a computerized system being developed for use within the FBI Identification Division that will eventually provide for automatic name and fingerprint searching.

arraignment—The judicial process by which an individual accused of a criminal offense is brought before a judge to enter a plea to the charge.

arrest record information—See Criminal Justice Information.

audit—The processes by which: a) the accuracy, completeness, and relevance of CCH record data are verified; b) CCH recordkeeping practices and CCH data are examined for compliance with applicable regulations. (See oversight.)

Comprehensive Data Systems Program—Launched in 1972 by LEAA, this program finances the development of State systems to standardize, integrate, and centralize the assembly and processing of criminal justice statistical data. Each system must include capability to track offenders through the criminal justice process and exchange criminal history records with other jurisdictions.

CCH—Computerized Criminal History—A record, maintained in machine-readable form, which contains information collected by a criminal justice agency on an individual and which includes: identification record information, arrest record information, criminal record information, and/or disposition information. (See "criminal justice information" for definitions of these terms.) An individual whose recorded charges were filed within a single State is represented by a "single-State" CCH record. If the charges were filed in more than one State, the entries comprise a "multi-State" CCH record.

correctional and reIease information—See Criminal Justice Information.

Criminal History Record Information System—A system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation, and/or dissemination of criminal history record information. The Department of Justice criminal history record information system encompasses the Identification Division and the Computerized Criminal History (CCH) fiIe systems operated by the FBI.

criminal intelligence information—See Criminal Justice Information.

criminal investigative information—See Criminal Justice Information.

criminal justice agency—a) any court with criminal jurisdiction; b) a government agency or any subunit thereof which, pursuant to statute or executive order, has responsibilities involving the apprehension, detention, pretrial release, post-trial release, prosecution, defense, adjudication, or rehabilitation of accused individuals and/or convicted offenders.

criminal justice information—includes any or all of the following:

a) Identification record—information describing an individual that does not suggest he has committed a crime—e.g., voiceprints, photographs, fingerprints.

b) Arrest record—information concerning the arrest and charging of an individual who has been accused of **a** criminal offense. Arrest record information does not include any reference to disposition of charge(s).

c) Criminal record—when disposition information is added to an arrest record, it becomes a "criminal record" (sometimes called a conviction record).

d) Disposition—a record entry or entries disclosing 1) that a decision has been made not to bring criminal charges against the subject of the record, or 2) that criminal proceedings have been concluded, abandoned, or indefinitely postponed. If an individual is convicted and sentenced, the related disposition information includes the nature of the sentence and subsequent events—e.g., release from correctional supervision, the outcome of appellate review, and/or executive clemency action.

e) Correctional and release record—information on an individual compiled in connection with bail, pretrial or post-trial release proceedings, presentence investigations, and proceedings to determine the individual's physical or mental condition. The term also includes information on an inmate's participation in correctional /rehabilitative programs, as well as information related to probation/parole proceedings.

f) Criminal intelligence record—information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity.

g) Criminal investigative record—information on identifiable individuals compiled in the course of investigating specific criminal acts.

h) Wanted person record—identification record information on an individual against whom there is an outstanding arrest warrant.

criminal record information—See Criminal Justice Information.

data quality—A measure of the accuracy, recency, completeness, and validity of NCIC records.

dedicated system—A computer or terminal complex, managed by a criminal justice agency, and used entirely for a criminal justice data processing application.

disposition—See Criminal Justice Information,

distributed data processing (DDP)—An arrangement of computers and/or intelligent terminals that allows some processing to be done at a central Iocation and the rest at remote locations connected to the site by communications circuits. In the NCIC system, remote processing usually occurs at the State level, but there may also be some done within terminals operated by local criminal justice agencies.

dossier society—A society **in which computerized records are maintained on individual citizens and are used by government** to monitor citizen activities so as to discourage political dissent and other types of disapproved behavior.

downtime—The total time that a computer system is out of service because of system outages and/or maintenance. "Outage time" refers to downtime which is due solely to system/component failure.

expungement—In connection with NCIC records, this term has been used interchangeably with "purging" or "sealing" of record information. It may or may not mean that information has been physically destroyed.

FBI message-switching plan—A proposal, currently under review within the Department of Justice and Congress, which would alter the operation and architecture of the NCIC system. Basically, the plan calls for locating all single-State CCH records within the States originating these records and installing a computerized message-switching subsystem at the NCIC in Washington so that a user requesting information from such a record could be connected directly to the agency holding it.

flag-A proposed entry to the identification portion of SSORI and full CCH records. The flag would signify that a specified criminal justice agency wished to be informed if and when certain events occurred subsequently. For example, the flag could indicate that **a** parole or probation agency wanted to know if the subject of the record had been arrested prior to the termination of his parole or probation.

front-end controller—An interfacing device, pIaced between a computer and an associated communications network, which manages communications between the computer and remote terminals attached to the network circuits. This function generally includes, but is not limited to, initiation and termination of message transmission, error detection and control, routing of each message to its proper destination, and control of the message flow to prevent excessive transmission delays for specified types of messages and/or users. The front-end controller may also switch messages among multiple users of the network.

hit—A positive response to a request from an authorized user for an NCIC record. The response consists of either the text of the record (if it is held by the NCIC computer center) or an abbreviated summary containing a numeric code which identifies the State criminaI justice agency holding the full text.

identification record information—See Criminal Justice Information.

Justice Department Blueprint—The popular name of a plan for future development of the Nation's criminal justice information systems. A basic aim of this effort, which began in the fall of 1977 after consultation with the House Subcommittee on Civil and Constitutional Rights, is to achieve a consensus—among users, Congress, and publIc interest groups—regarding the

needs for and uses of the NCIC system.

LEAA—An acronym for the Law Enforcement Assistance Administration, a part of the Department of Justice. LEAA dispenses Federal funds to the States for criminal justice information systems and establishes many of the policies concerning their operation.

NCIC—An acronym for "National Crime Information Center, " the physical location within the FBI's Washington, D. C., headquarters of the NCIC system's central computer complex.

NCIC Advisory Policy Board—A 26-member group which makes recommendations concerning NCIC operations and procedures to the director of the system. The Board includes 20 representatives of local, State, and regional users, and six others appointed by the FBI.

NLETS—An acronym for "National Law Enforcement Telecommunications Systems, " a nationwide communication network operated by State law enforcement agencies, which provides them with the capability to exchange administrative messages. Exchange of full, single-State CCH records between States is part of the NLETS communications traffic stream.

node—The point where a communications network interconnects with access circuits to-/from a user's computer and/or terminal equipment. Typically, the node contains switching equipment designed to route messages among network users. The node may also include hardware/software to perform speed/code conversion, error-detection /control, and other communications-related functions.

oversight—The process by which Congress examines NCIC policies and practices to determine whether they comply with relevant legislation. (See audit.)

plea bargaining—The process of pleading guilty to a lesser charge in order to avoid standing trial for a more serious one.

pointer index—See "SSORI. "

Project SEARCH—A cooperative, 18-month Federal-State effort, begun in June 1969, to develop a prototype, online, computerized criminal history exchange system. A key feature of the design for SEARCH ("System for Electronic Analysis and Retrieval of Criminal Histories") was the use of the central index containing references to criminal history records stored within each participating State. A major goal of the project was to test the effectiveness of this index as a means of relating record inquiries to the actual records. In December 1970, when the SEARCH demonstration ended, Attorney General Mitchell authorized the FBI to take control of the index. This file became the nucleus of the present NCIC/CCH system. Project SEARCH was incorporated in 1974 as SEARCH Group, Inc., a research and policy advisory group representing present and prospective users of NCIC services. It includes participation of representatives from each of the .50 States and 3 territories.

purging—As used in connection with NCIC records, this term means the complete removal of information concerning an individual from access, via either routine or special access procedures. Purged information is not necessarily destroyed. However, a recommendation to make destruction mandatory for purged records has been proposed by the Committee on Security and Privacy of SEARCH Group, Inc.

rap sheet—Synonymous with "arrest record. "

response time—A measurement of the speed with which inquiries can be answered by an online information system. The response time measurement generally begins with the instant the first message character leaves the inquiring terminal and ends when the last character of the answer is received by that terminal.

sealing—As used in connection with NCIC records, sealing means the removal of information concerning an individual from routinely available access. The information remains available but only through special access procedures. (See also: "expungement," "purging".)

SSORI—An acronym for the proposed "Single State Offender Record Index," central ("pointer") index proposed to be incorporated into the NCIC/CCH file under the FBI's proposed limited message switching implementation plan. The SSORI file would contain a physical description, and possibly information on the first arrest, of each individual represented by a single-State NCIC/CCH record. Complete details of each such record would be stored in the State which compiled it. When NCIC received a CCH inquiry, the SSORI file would be searched automatically to determine whether a single-State CCH record, relating to the subject of the inquiry, was in any State file. If such a record was found, the inquiring agency would be so informed and could then obtain a copy by communicating directly with the "holding" State.

stakeholders—As applied to NCIC, the **term** means individuals or groups whose interests will be materially affected by the manner in which the system is operated and/or its records are used.

wanted person information—See Criminal Justice Information.

0